Copyright Image; Visual Digital Metadata Compliant Application Innovation Design

Ellyana Mohd Muslim Tan[1], Ruslan Abdul Rahim[2], Md Nagib Padil[3], Noraziah Mohd Razali[4]

[1,4] Universiti Teknologi MARA (UiTM), Cawangan Sarawak, 96400 Mukah Sarawak,
[2] Faculty of Art & Design, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor, Malaysia
[3] Universiti Teknologi MARA (UiTM), Cawangan Perak, Bandar Baru Seri Iskandar,
32610 Seri Iskandar, Perak

ellyana@sarawak.uitm.edu.my, ruslan@uitm.edu.my, nagib746@uitm.edu.my,
noraziahmohdrazali@uitm.edu.my

Abstract — This research proposes a system for securely registering an image to its creator or owner, in order to curtail image theft across the internet. Current strategies for curtailing theft include Watermarking which this can be visually unappealing, and can be overcome with image editing software, or by cropping. Metadata which creator information can be attached to images with metadata, but unfortunately can be easily changed after the fact with software. This research proposes a new strategy. Any image creation device that connects to the internet, such as a smartphone or a camera with IoT (internet of things) technology, can upload a copy of that image to a secure image vault at or near the time of creation; before the image is transferred off of the device. This allows the image to be irrevocably associated with the person who created it.

Keywords – Creativity, design course, fashion, silhouette and visual data

1. Introduction

In this era of social media and ubiquitous internet access, sharing digital images is extremely easy. Equally easy is copying an image from a website, saving it, possibly altering it, and then sharing it without permission of the owner of the image. One method of determining image ownership involves examination of the metadata stored within a digital image. Limited metadata is often added to images automatically by digital photography equipment such as smartphones, laptops, and cameras. Metadata keeps Extended File Information (EXIF) for several image formats, including the Join Photographic Experts Group (JPEG) file format, Tagged Image File Format (TIFF) and RAW file. The EXIF data keeps technical tags including Flash Used, Focal Length, Exposure Time, Aperture or Focus No, Shutter Speed and Distance, as well as administrative and digital rights data, which can include the image creator and contact information as well as copyright information. Unfortunately, this data is not secure--many software tools exist to allow easy alteration of metadata associated with an image, as well as the image itself. Stolen images often are stripped of identifying metadata first. In work conducted by David E. (2006) and Kamaruzaman, M. F., & Zainol, I. H. (2012), photo images are protected by using the Stenography formula; a "watermarked" formula that has been in use for several years. This formula is being utilised as one of the methods of regulating the change of information. Other than that, another information hiding formula that are being used include a number of watermarking digital innovation such as cryptography. Nevertheless, Steganography can easily fail if the existence of secret information is revealed. Whereas, in watermarking, the existing information appears and able to be recognised while the cryptography can be manipulating with appropriate keys.

2. Research Objective

The objective of this study is to provide a better system of digital rights management for the photographer or image creator/owner, as well as any subsequent rights holder of images. Protection is achieved by transmitting photos to a global image vault, accessible via the internet, importantly before the image can be transferred from of the image creation device, such as a camera or smartphone.

3. Handling and structuring digital imaging

Latest element of data system

Referring to the US Patent document entitled "Associating Data with Images in Imaging Systems" by Davis et al (2006), structure digital imaging utilizes metadata server where the image information is convertible in accordance with compliant and non-compliant application. Based on the figure 1 as shiown below:

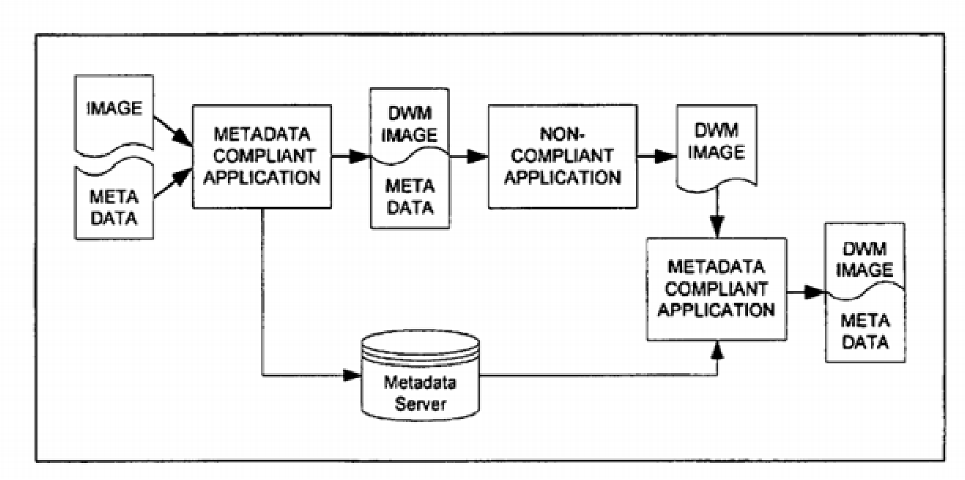
IMAGE
META DATA
METADATA COMPLIANT APPLICATION
DWM IMAGE
META DATA
NON-COMPLIANT APPLICATION
DWM IMAGE
METADATA COMPLIANT APPLICATION
DWM IMAGE
META DATA
Metadata Server

Figure 1. Until today, the data transfer system has been controlling metadata technically only, which is inconsistent with the digital watermarking.

Proposal Methodology of Information

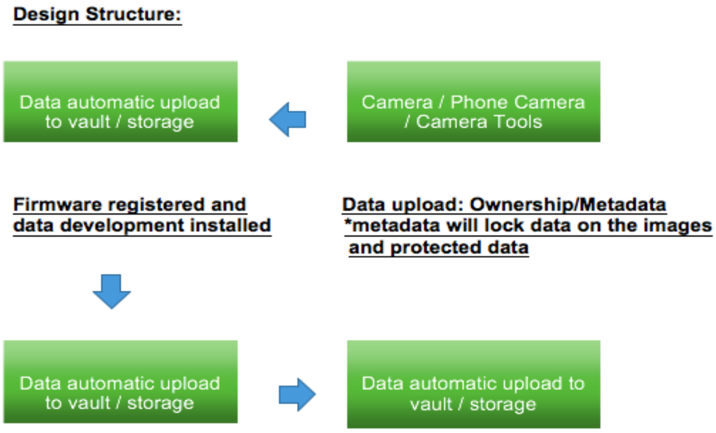
Design Structure:
Data automatic upload to vault / storage
Camera / Phone Camera / Camera Tools
Firmware registered and data development installed
Data upload: Ownership/Metadata *metadata will lock data on the images and protected data
Data automatic upload to vault / storage
Data automatic upload to vault / storage

Figure 2. Latest enhanced system will control images and data via the vault bank image and will utilise the Neural Engine Chip method along with metadata control. The purpose is to detect whether the ownership copyright and image usage are more organised.

4. Suggestion of DNA Digital Image Data

The enhancement of AI expands the photography technology to an advanced level. For example, in the early year of 2018, the use of Al-Centric has introduced Bionic Neural Engine Chip, which is a chip that has been designed specifically for certain tasks such as image–and-face–recognition and AR application. The Bionic Neural Engine Chip was first used by Apple company and followed by a few technology companies such as Google, which is the line pixel google application, including China smartphone technology such as Huawei; the P20 Pro. This chip has the capability of accommodating small sensors such as image control via a drone or mirrorless camera. Evgeny Tchebotarev, in his article, "AI Is Already Changing the Way We Think about Photography", states that by using Bionic Neural Engine Chip, DSLR would be far left behind. It is critical that the image is transmitted directly to the vault from the image creation device to ensure that the metadata attached to the image has not been manipulated. Removing a flash card from a camera, for example, would make it impossible to upload images on that card to the vault. The image creation device must have the ability to write metadata to the image including the image creator, his unique vault ID, and copyright information. That way, when the image is added to the vault, it is forever associated with its creator/owner. Once the image is in the vault, the vault can then be used in the following ways to ensure digital rights:

(1) Secure Publishing - when an image is published on a website or on social media, the owner of the image can publish directly from the photo vault. The site where the image has been published would be aware it originated from the secure vault and can place a visual indicator that this is a "verified image" and possibly include copyright information provided by the vault with the image. Thus, viewers of the published image would be certain of the origin of the image they are viewing.

(2) Secure - *flexible rights management - when an image is sold or digital rights are otherwise transferred to or shared with a third party (who also has a unique vault ID), the owner of the image would log into the image vault and register the transfers. Rights associated with the transfer would be made explicit. An image may be transferred completely to a new party (an* ownership change), or a more limited license to use the image might be specified. The limit might be that the image can only be published on specified domains. Thus, if the third party attempts to post an image on facebook when the transfer only allows publication to instagram, the upload to facebook from the vault would be rejected. In addition, the purchaser of rights to the image is assured that they are not purchasing a stolen image. A full history of the digital rights to an image would be maintained in the vault in perpetuity.

(3) Image search - not all images that are published or sold will be in the vault. And once an image leaves the vault and ends up on the internet, there is still no guarantee that it will not be stolen and published elsewhere, or resold. When an image is being considered for publication or rights transfer that does not originate from the vault, the transferee can nonetheless search the vault for an image match. The technology exists for image searches based upon mathematical relationships within the image as well as metadata if it has not been removed. Google, for example, has provided a search by image function since 2010. While this sort of search may produce false matches, especially for commonly photographed images, or may not match an image that has been significantly altered, it can at least provide some assurance to the transferee that the image they are receiving is not already published online.

(4) Social Media Authenticity - a common problem is the creation of fake profiles on social media or dating websites in order to deceive other users. These profiles often use photos stolen from other profiles or websites. To assure users they are viewing an authentic profile, social media sites might require a user to provide his vault ID, and ensure that the photo posted comes his own vault. Or even if not required by the site, when a user posts a photo, they might select a "verified photo" option, to confirm that the selected photo came from their personal vault. This can provide some assurance that the photo is likely to be authentic.

(5) Version Control of Images - images are, of course, often manipulated by their owners with image editing software for legitimate reasons. And these edited images are often published or sold. Thus Image editing software, such as Photoshop, should integrate with the vault, in order to allow the owner to save an edited version of the image in the vault (Rani, N. M., Zainol, I. H., & Kamaruzaman, M. F. 2015). When editing vault images, ad-hoc metadata changes would not be allowed. Any metadata changes would be managed by the software consistent with vault rules. All edited images will refer back to the source image they from which they derive, providing a complete history of edits of an image.

Conclusion

Based on the observation, the AI Technology is able to yield tracing data and able to control ownership. With this system, its use is limited to the mobile technology, but also for any other types of networking. It is safe and reliable in assisting widespread of image misuse without permission.

References

Bruce L. Davis, Lake Oswego, Geoffrey B. Rhoads, West Linn, William Y. Conwell, (2006) Associating Data With Images In Imaging Systems Portland, United States Patent, Mar. 7,

Bruce L. Davis, Lake Oswego, Geoffrey B. Rhoads, West Linn, William Y. Conwell (2007) Authenticating Metadata And Embedding Metadata An Watermarks of Media Signals, Portland, United States Patent, Apr. 24,

Feng-Hsing Wang, Jeng-Shyang Pan, Lakhmi C. Jain, Digital Watermarking Techniques**,** Studies in Computational Intelligence book series (SCI, volume 232)

Jessica Fridrich, a Miroslav Goljan, and b David Soukal (2018) Searching for the Stego-Key, Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. **5306**: 70–82. Retrieved 5 June 2018.

Kamaruzaman, M. F., & Zainol, I. H. (2012). Behavior response among secondary school student's development towards mobile learning application. In 2012 IEEE Colloquium on Humanities, Science and Engineering (CHUSER), (pp. 589-592).

Metadata Working Group, Guidelines for Handling Image Metadata, © Copyright 2008, 2009, 2010 by Adobe Systems Inc., Apple Inc., Canon Inc., Microsoft Corp., Nokia Corp. and Sony Corp. All rights reserved.

Paul Alvarez, Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis, International Journal of Digital Evidence Winter 2004, Volume 2, Issue 3.

Rani, N. M., Zainol, I. H., & Kamaruzaman, M. F. (2015). Empirical study on game-based learning phenomenon through mobile design technology. In International Colloquium of Art and Design Education Research (i-CADER 2014) (pp. 195-199). Springer, Singapore.