Digital Image Misused Protection and Tracking Techniques and Tools

Nor Azlina Abd Rahman[1], Mohamad Amirizal[2] and Nursyafiqah Hanis[3]
[1,2,3]Faculty of Computing, Engineering & Technology, Asia Pacific University of Technology & Innovation, 57000 Kuala Lumpur, Malaysia
[1]nor_azlina@apu.edu.my

Abstract— **This research focuses on several issues that commonly faced by the Social Media users. Apart from that, discussion on security and awareness that can be considered by the Social Media users to protect their data when uploaded to the Social Media is also included. Data protection mainly covered on digital images and techniques or tools that can be used to protect digital images from being misused by unauthorised party. Detail discussion on how Digital watermarking can be used to the digital images in providing security to users were discussed. Several tools are highlighted such as Copyscape and TinEye that can be used to track of any images misused by unauthorised party.**

Index Terms—**digital images, image misused, digital image security, digital watermarking, Copyscape and TinEye**

1. Introduction

Social media, a widely known medium for communication and information sharing. In this past few years, social media has exploded on the internet due to the vast features it provides toward the community. Some of the features includes boundless interaction between user, content sharing and even collaboration between user (Rouse, 2013). This has also become a medium for businesses to further expanding their market by promoting the product on the social media. To further elaborate, sharing images has been one of the most use features on social media.

Although the existence of social media has been totally positive, the facts that social media security and privacy has been neglect by user has been a concern due to cases arise from it. Identity theft, image stealing and forgery, unauthorized access to user account and piracy of image has been some of the example of by-products of lack in knowledge of social media security. It is a very common situation for a user to never look beyond the original security and privacy setting of their social media accounts (Search Security and Syngress, 2016). The aim of this paper is to discuss on social media security and to create an awareness amongst the social media community and to further elaborate and discuss on how to protect social media account user images from being misuse and security features that is provided by social media websites.

2. Digital Watermarking, Can They Prevent Misused of Images

This part should contain sufficient detail so that all procedures can be repeated. It can be divided into subsections if several methods are described.

Image is an optical counterpart or the appearance of an object, as is produced by reflection from a mirror, refracted by a lens, or the passage of luminous rays through a small aperture and their reception on a surface (Rouse, 2013). Images have been used widely for many purposes since the first camera invented. From art, educational, medical and conventional purposes, images have assisted every individual and organization to perform their daily tasks. Throughout the line of development, image use has been evolved. Nowadays image can be a powerful tool, profitable item and reliable references. Due to the reliability of an image, some see it as an opportunity to misuse it for their own benefit.

Digital watermark is a visible or invisible identification code that is permanently embedded in the host media (Search Security and Syngress, 2016). It's also used for the security of the digital content and to protect the data from illegal users and provides the ownership right for the digital data. Every image or media contents got its own copyright information, where his kind information will be unseen and hidden directly in the images or media content by applying an invisible watermark. Invisible watermarking applied cannot be removed by the user and prevent them from unauthorized copying and alteration, but it can be extracted or read by the appropriate party and under specific conditions. Embedding watermark into the content must be unseen and not affecting the quality of the content. Moreover, the digital watermarking must be vigorous to media manipulation, tampering and attacks (Search Security and Syngress, 2016). Digital watermarking technique involves two kinds of algorithm: one as the embedding

and the other is detecting algorithm. Figure 1 & 2 illustrates the processes involve in embedding and detection algorithm.

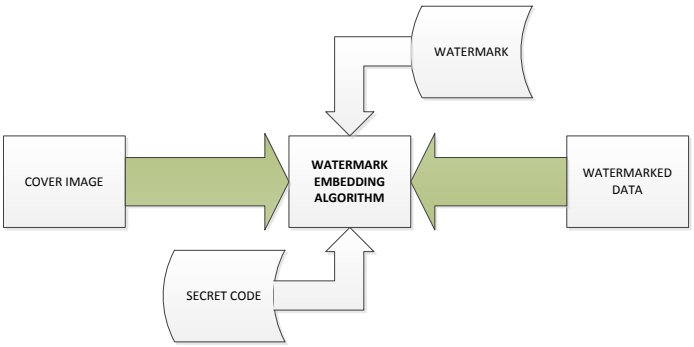

Figure 1: Watermark embedding process (Search Security and Syngress, 2016)

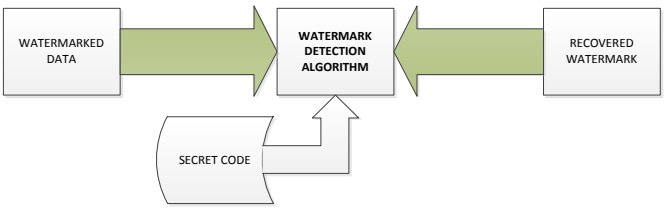

Figure 2: Watermark detection process (Search Security and Syngress, 2016)

Invisible information in digital watermarking only can be extracted by using dedicated detector or extractor. After the embedding process is completed, the watermarked image became more vigorous against attacks. Normally digital image watermarking works in three stages, embedding, distortion/attack and detection/retrieval stage. The summarized figure of digital image watermarking stages is shown in Figure 3.

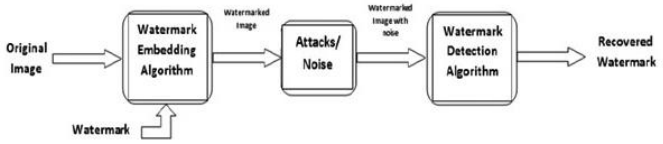

Figure 3: Digital watermarking image stages (Search Security and Syngress, 2016)

There are various techniques can be applied in digital watermarking. The techniques usually applied can work on two domains, either spatial or transform domain. The spatial domain technique works directly on pixels, where watermarks being embedded by modifying the pixel value. Least Significant Bit (LSB) is the most commonly used spatial domain technique. While transform domain technique aim is to embed the watermarks in the spectral coefficients of the image. Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation and Discrete Fourier transformation are the most commonly used transform domain techniques.

The simplest digital watermarking technique is Least Bit Significant (LSB) under spatial domain technique, where watermarks being embedded at the least significant bit of some randomly selected pixel of the cover image. This technique is easy to apply and it provides high perceptual transparency where it does not degrade the cover image quality. Even though this technique is very much unnoticeable, due to its poor robustness, this technique is vulnerable to attacks.

As for transform domain techniques, Discrete Cosine Transformation (DCT) used for the signal processing where it transforms a signal from a spatial domain to frequency domain. Every field of image processing, data compression and pattern recognition use DCT. DCT watermarking is better than spatial domain technique in terms of robustness against simple image processing like low pass filtering, contrast and brightness adjustment. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image (Pakya, 2016). The process in applying DCT for embedding process involves division of frequency upon the cover image. It will be divided into 3 types of frequency that are low, medium and high. As shown in Figure 4, where FL is the low frequency region, FM is the medium frequency region and FH is the high frequency region. Usually the medium frequency region is being selected for embedding process, where the boxes are in grey coloured. The grey coloured area represents the perceptually significant portion of the image.

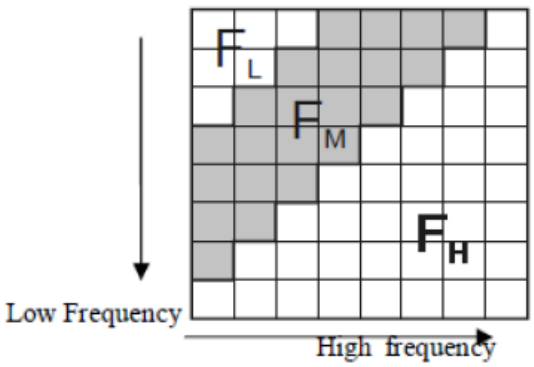

Figure 4: Discrete Cosine Transform Region (Pakya, 2016)

Discrete Wavelet Transform (DWT) is another technique can be used under transform domain where this technique is much more complex than DCT. It requires longer computation time and higher computation cost. Unlike DCT, DWT divides the images into high frequency quadrants and low frequency quadrants. The low frequency quadrants again will be divided into two parts as before repeatedly until the image is entirely decomposed. DWT is widely used in digital watermarking because of its excellent spatial localization and multi resolution techniques (Search Security and Syngress, 2016). The watermark embedding process involves alpha blending technique. It blends both DWT applied on cover image and the watermark image to become a watermarked image. Summarized figure of watermark embedding is shown as Figure 5.

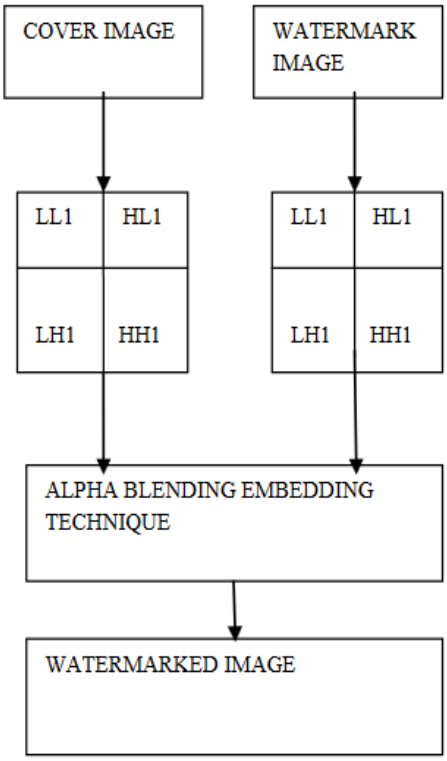

Figure 5: Watermark embedding technique after DWT applied (Search Security and Syngress, 2016)

Another technique can be applied under transform domain is Discrete Fourier Transform (DFT). DFT also use decomposition. The decomposition of an image is in sine and cosine form. Two types of DFT based watermark embedding are direct embedding and template based embedding techniques. Direct embedding technique the watermark is embedded by modifying DFT magnitude and phase coefficient. While template based technique introduces the concept of templates. DFT is vigorous against geometric attacks like cropping, scaling and rotation. DFT also rarely used due to its complex output value and it requires more frequency rates. Moreover, this technique computational efficiency is very poor.

As a conclusion, various techniques offer in digital watermarking could partially avoid image misuse because it still can't prevent the copying and distributing misuse activity. Though it still protects the copyright and information of an images, a thorough research in future is essential in order to develop truly robust, transparent and secure watermarking technique for images.

3. Tips to Prevent from Image Misused

Sharing images online about user or what they like or currently doing has becoming a trend for social media community. A selfie taken or a photo by photographer is share in social media is mostly likely for personal gains or to promote the business that they are currently into (Siciliano, 2014). Either way, having user image stolen from you and republish on other websites without crediting it to user has become troublesome and can be consider as stealing or copyright infringement.

This section will discuss on some of the tips to be taken into consideration to prevent any image misuse or identity theft on social media. The most basic things user can do is to always be alert on social media and to configure properly their privacy setting (Siciliano, 2014). Most of the social media websites do provide privacy setting for user accounts so that they can configure their account based on their desire (Siciliano, 2014). Taking Facebook as an example, in their privacy setting it includes the setting of what type of user can see the images of post that the user share. The setting goes to either making it public, making it available to only friend or to be only accessible by user (Siciliano, 2014). As this setting goes to generally for the user account and can also be modified based on the type of post every time user share something, user should make full use of this features by limiting the post of images only to their friends (Siciliano, 2014). This setting leads to another point which is to be selective on approving friend in social media. Generally, only approve or accept friend request from people that user knows rather than simply approving them (Pakya, 2016).

If users are trying to expand their social circle, only make or approve request from valid account. There are several ways to identify if the account is fake and one of it is to see the date that the account was created in conjunction with the user information provided (Pakya, 2016). A newly created account with an unorganized basic information might point toward that the account is a fake account (Pakya, 2016). Social media user also

should be aware that their social media account might be linked up with one another and posting an image on one social media site may leads to posting the same image on other social media sites (Pakya, 2016). With this in mind user can either have the same level of privacy setting across all of their social media accounts or to unchain their social media account with one another.

Next tips that can be used to prevent image misused on social media is to make it difficult to use the image without owner's permission (Wright, 2015). As complicated as its sound, there are several ways to make user image difficult to be stolen. One of it is to disable the right click option on user's images (Ewer, 2014). Taking WordPress for example, upon setting up the sites there is a plugin provided that will block the ability of right click on the sites (Ewer, 2014). This plugin will block any right click attempts on images thus rendering the save image option on the contextual menu. Combining this with an option to select "none" on a "link to" option when uploading an image will block any unauthorized or misused of user images (Ewer, 2014).

Another point to add to this is to provide watermark or user signature on the image uploaded (Ewer, 2014). This will notify other user that the image is solely belongs to the user and that it is not to be wrongfully distributed and misused (Ewer, 2014). Traditional less aggressive watermark will allow more experience user to just crop out the watermark image, thus in opinion we suggest that user perform a full semi-transparent watermark (Ewer, 2014). Taking again WordPress as an example, they provide plugins which embed watermark over the image upon uploading. This will not alter the image resolution and make it difficult for other user to crop out the watermarks (Ewer, 2014). This type of watermark is commonly seen with images originated from iStockPhoto and GettyImages.

Final tips that can be used by social media user is to configure the metadata of your images (Ewer, 2014). Metadata is great because unless it is remove by user themselves, they are permanently attach to the image (Ewer, 2014). This is a great feature for image uploader on social websites as the metadata will keep track of user camera technical data and contains user copyright information. The relationship between the metadata and user copyright lies in the user camera itself (Ewer, 2014). Today's camera will directly inject a metadata into the images itself via the camera configuration (Ewer, 2014). Typically, user can add several lines of text which includes copyright and name upon the injection of metadata while processing the images.

For serious user that wanted to keep their photo in check, they can use google alerts tools to help them further protect their image (Ewer, 2014). Google alerts helps you set up keyword triggers that sends user an email based upon the criteria that user has specify. In other word google alerts provide protection by monitoring the web based on the content specify (Ewer, 2014).

In conclusion, several tips provided may save user images from harm. With a few easy steps users can really make a difference in preventing their images from being uncredited or, even worse, redistributed online without knowledge. Passive tools like embedding a metadata or using google alerts will assist a lot in monitoring of unauthorized use of user's image.

4. Image Misused Tracking Tools

Images, sharing them or posting them on social media is unavoidable. This also lead to the fact that once user posted up their images the risk of the image being stolen and misused are increases, but what other medium can be taken by user to show their creativity, artwork and masterpiece. There is a simple way to post up user images on social media and still avoid any misused or unauthorized use by it.

This section will discuss on how user can upload their images on social media but still keep it out from being misused by another user. One of the way is to use available online tool to detect users publish images whether or not they are being misused. They are several tools available online although some of it is not free. One of it is called Copyscap (Hines, 2012). This is rather a good option for those users who are frequently uploading their images (Hines, 2012). To use these tools is rather simple and even user friendly for normal user. All user has to do is to paste their websites URL and Copyscape will generate a result based on which ever site that has been reposting user photo without their authorization (Hines, 2012). Getting full scale premium result is going to cost on these tools but it is worth it comparing to the loss that user has to suffer due to their images being misused or unknowingly republished (Hines, 2012).

The following will show you a step on how to detect misused image by surfing it on Copyscape. Firstly, go to the websites to start the process (**Figure 6**).

Figure 6: Copyscape main page (Hines, 2012).

Next is to fill in the search bar with user own URL to check on whether other websites are using the images from user published image and click on go. Finally check and see whether there are any websites or post that user should be concerned about (**Figure 7**).

Figure 7: Copyscape Search Results (Hines, 2012).

One other tools or plugins that are available for user to use in order to track their images is trackback notifications (Hines, 2012). Trackback is a tool that enable user to receive alerts as soon as another user hot links your post (Hines, 2012). Typically, there is a high chance that a frequent site linking by other user might prove that the users are copying and reposting the original site images. Trackback is easy to use, user just simple need to check back visitor's feedback and then lookout for any websites or user that seems suspicious (Hines, 2012).

In the early of 2016, there has been a cased where a professional photographer images has been posted for an online contest without the knowing or authorization from the owner himself (Peters, 2016). Richard peter claims that the images were taken several years back and unknowingly use to enter a completion one of Dutch publication and as the result the image has won a total of 250 euro not only for the current month publication but few months back with some different types of images (Peters, 2016). Unsatisfied by this action he called up the author to notice them about it and start up doing research whether or not his other images are being misused.

In this case, he uses a reverse image search tool to find other images of his that are being posted without his knowing. This tool is call TinEye (Peters, 2016). What this tool basically do is to find visually same images of the original images on the web. This will enable user to find out whether the images they posted has been wrongfully misused (Peters, 2016). This tools also come with additional features which include the ability to register user images along with the ability to find out the origin of images and how it is being used and whether exist any modify version of it.

The predecessor of TinEye is one of the product by one of the giant company call the google image (Peters, 2016). In google images user can conduct a reverse image search by providing the original images. This will produce a result which includes every related images or visually the same images as the original (Sacino, 2016). This is possible through the pixel search provided by google images. The special algorithm is the one in charge to find the similar images as the original (Sacino, 2016). How to use these tools is simple, user can enter google image page and drag and drop their original image onto the search box and see the results.

In conclusion being unaware of the state of your image can be a really harsh thing. Thus, being smart and aware of how your photo is being used or whether they have been wrongfully used can prove to be an advantage for user. Available tools like Copyscape and technique such as reverse image search might have a great impact upon user on helping user to prevent image piracy.

5. Other Security Techniques to Avoid Image Misused

This section discusses on several techniques that can be considered to avoid from Image misused

5.1 Changing Password

Password is a common security features provided by social media and is a compulsory feature. Changing password is also a feature provide to social media user which can be used freely whenever a user feels like their password is compromise. It has become a norm to social media community that frequent changing of password provides a more secure account and strong security, but thus changing password really provide a stronger security.

In this section we will discuss on what happens when user changes their password, the impact of the frequent changing of password and when would it be appropriate to change user password. Unless user have the reason to think that their password has been compromise, changing password might do more harm than good (Peterson, 2016). In other words, changing password often might not have any security difference (Peterson, 2016). Although passwords are commonly kept in hash format which made it difficult to crack, the strength of the password is already weak to begin with. Combination of name and date of birth are the common method use by user to create their password (Peterson, 2016). When require to change their password, user normally tend to use the same password but with a different mixture such as changing "admin1505" into "aDmin1505" which can be easily guess (Goodin, 2016). This provides a slight or

none impact towards security due to the changes can be guess easily if they are compare towards the original or previous password (Goodin, 2016). Changing password gives a great impact to user making them to produce lesser and lesser secure password and a more predictable pattern of password changing (Goodin, 2016).

The provided fact gives out the image that changing password is not even needed if users have a strong password (Cranor, 2016). This is might not be the usual cases as there is a time that user is needed to change their password. This case happens when user provides a weak password to begin with (Cranor, 2016). Other cases include users just being trick by phishing websites, observing a strange behaviour on their social media account, and when user notice that they are being shoulder surf when they are typing their password (Cranor, 2016).

In conclusion, changing password frequently might not provide more security compare what to what user normally thinks. Changing it frequently only make user to provide less strong and predictable password. It is advised for user to change their password only when they feel compromise and to provide a strong password to begin with.

5.2 Staying Away from Social Media

Social media issue such as image theft and identity theft has been rather concerning to some of the community. Questions like is my image safe, are they being stolen, is the user account that they obtain has been compromise and misused and are there any accounts created by their name has been used on different social media websites. The question will somehow cross through user minds and ultimately leads to whether the only way to avoid this and the solution to this concerning matter is to stay away from social media.

In this modern society staying away from social media is not an option as they need to use basic communication medium such as email account. Are there any other ways to avoid images from being misused on social media, yes, as there are no absolute ways to prevent image piracy, user can always take a preventive measure in order to reduce or even to avoid any piracy. One of the way is to register through a non-profit organization call Creative Commons (Stumpf, 2013). This organization provide easy to use copyright license which is standardized and simple (Stumpf, 2013). They also provide conditions for sharing users content online and enable user to switch between default copyright terms of all rights reserved or to some rights reserved.

The other way is by changing the default privacy setting impost by most of the social media websites (Panda Security, 2013). Most of the websites default general setting is used to maximize the experience user get on the social site, but highest experience does not mean that everything is properly configure (Panda Security, 2013). Some of the setting that user can change is by having limitation on user post to only friends. In conjunction with this configuration, user can also resize their image so that the other user can only view a souvenir version of it (Plagiarism Today, 2014).

If users are professional photographer or in the way of becoming a professional photographer, it is advisable that they do not post photo they taken directly onto the social media but instead post it on user's privates websites and post a link of it on social media linking it (Plagiarism Today, 2014). This method can be further being image piracy proof by having their private websites enabling plugins such as right click disable which will provides a really great help (Roe, 2013). What this will do is that every time visitor uses right click on the image the contextual menu would not pop up, instead an error message will be pointed out for the user (Roe, 2013). On user private website, they can also provide a layer of semi-transparent watermark which will cover the whole of their image and show that the artwork is not to be shared without permission (Roe, 2013). This method can be implemented through plugins on sites such as WordPress which will cover the image with semi-transparent watermark upon uploading the image.

In a nutshell, keeping away from social media might be the last resorts if users' photo is kept on being pirated as there are several ways to avoid images from being misused. Understanding the concept of privacy and executing some preventive way might be the best options for user to prevent their work of art to be ever being pirated.

6. Conclusions

In this paper researcher have discuss on several key factor that influence social media user to be a target of hacking attacks. The research main focus of topic is on image piracy and theft and has discuss on several methods to be used in order to avoid image theft. The discussion also focusses on digital watermarking and how can it benefit social media user. Extensive research has also been done in order to know whether staying away from social media is the only way to avoid image theft.

Acknowledgments

The authors wish to express gratitude to the management of Asia Pacific University for their support.

References

Cranor, L. (2016), *Federal Trade Commision*. Retrieved January 9, 2018 from https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

Goodin, D. (2016), *ARS Technica*. Retrieved January 9, 2018 from http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/.

Ewer, T. (2014), *GRAPH PAPER PRESS*. Retrieved January 6, 2018 from https://graphpaperpress.com/blog/protect-website-image-stealing/.

Hines, K. (2012), *Kissmetrics Blog*. Retrieved January 7, 2018 from https://blog.kissmetrics.com/content-scrapers/.

Pakya (2016), *BusinessZone*. Retrieved January 5, 2018 from http://www.businesszone.co.uk/community/blogs/pakya/tips-to-prevent-identity-theft-from-social-media.

Panda Security (2013), *Panda Security*. Retrieved January 11 2018 from http://www.pandasecurity.com/mediacenter/social-media/5-tips-protect-photos-facebook/.

Peters, R. (2016*), Richard Peters Photography*. Retrieved January 7, 2018 from http://www.richardpeters.co.uk/blog/2010/08/04/image-theft-find-out-if-yours-have-been-misused/.

Peterson, A. (2016), *The Washington Post*. Retrieved January 8, 2018 from https://www.washingtonpost.com/news/the-switch/wp/2016/03/02/the-case-against-the-most-annoying-security-measure-virtually-every-workplace-uses/?utm_term=.397d66863ea5.

Plagiarism Today (2014), *Plagiarism Today*. Retrieved January 11, 2018 from https://www.plagiarismtoday.com/2014/08/28/size-online-images-uploaded-avoid-theft/.

Rohler, N. (2016), *DWUser.com*. Retrieved January 11, 2018 from http://www.dwuser.com/education/content/stop-the-thieves-strategies-to-protect-your-images/.

Rose, O. (2013), *Kissmetrics Blog*. Retrieved January 7, 2018 from https://blog.kissmetrics.com/find-remove-stolen-content/.

Rouse, M. (2013), *WhatIs*. Retrieved January 2, 2018, from http://whatis.techtarget.com/definition/social-media

Sacino, E. (2016), *Picture Correct*. Retrieved January 7, 2018 from http://www.picturecorrect.com/tips/how-to-protect-your-photography-online/.

Search Security and Syngress (2016), *TechTarget*. Retrieved January 2, 2018 from http://searchsecurity.techtarget.com/feature/Social-Media-Security.

Siciliano, R. (2014), *Securing Tomorrow. Today*. Retrieved January 5, 2018 from https://securingtomorrow.mcafee.com/consumer/family-safety/10-tips-protect-social-networks/.

Stumpf, E. (2013), *The Press Enterprise*. Retrieved January 11, 2018 from http://www.pe.com/articles/images-661336-website-image.html.

Wright, C. E. (2015), *Lynda.com*. Retrieved January 6, 2018 from https://www.lynda.com/articles/3-ways-protect-online-images.