ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

Survey on Image Security in Social Media using Digital Watermarking with Embedded Metadata

Bilal Sayyad[1], Mubarak Sache[2], Vaseemakram Sayyed[3], Prof. Sonali Patil[4]

U.G. Student, Department of Computer Engineering, AAEMF's College of Engineering, Pune, Maharashtra, India[1, 2, 3]

Asst. Professor, Department of Computer Engineering, AAEMF's College of Engineering, Pune, Maharashtra, India[4]

ABSTRACT: Users on social media increases day by day,because of this reason the images uploaded in social media increases.There are many problematic issues occurs if no precautions were taken at the time of uploading image in social media. Currently various issues arises like unauthorized sharing of photo over the Internet, ownership, identity fraud and tarnished data from image. To solve these problems our proposed solution is by using digital watermarking with embedded metadata. To increase the security of digital watermarking technique, extract the useful metadata of the image which are used for embedded information for watermarking process. An Android application to be developed for applying the visible and invisible watermarking algorithms, and other experiments and analysis. These watermarked images will be uploaded in four various social media sites, and then checked presence or changes to, the embedded metadata for each of the watermarking techniques and also detect tamper images.

KEYWORDS: Image security; social media; digital watermarking; embedded metadata; digital image tampering detecting.

I. INTRODUCTION

Social media is a collection of online interactive communication channel that allow users to create and share information, and participate in social networking [8]. Various Types of social media includes Insatgram, Twitter, Facebook, and WhatsApp. Every year, the number of social media users increase rapidly, and based on a survey done by Statista.com [7], an online statistics company that handles market research and business intelligence, stated that the number of social media users exceeded 1.79 billion users worldwide in 2016.

Digital images being the natural carriers of information are the most widely accepted and convenient way for expressing and transmitting information. As per the statistics, in 2013 on an average 350 million images and in 2014, 1.8 billion digital images were uploaded to Facebook every single day indicating that more than 20,000 images make their way on internet every single minute [1].The rapid increase of users, along with the enhanced technology in digital photography, has led to an increase in the numbers of images uploaded into social media. Furthermore, apart from individuals, companies looking to market their products and even news agencies are also joining this social media bandwagon to increase their presence and profit. As the number of users and images increase, new issues arise. These issues include image ownership issues, sensitive image copied over cyberspace, identity fraud, and metadata removal. Consequently, in order to solve these problems, this research is conducted and the solution to embed metadata into images as watermark is proposed.

Due to of this wide circulation of the images on the net and with the help of readily available image editing software's, these digital images can easily be altered or manipulated in order to misguide the common masses. Thus, the tampering of a digital image means the intentional manipulation of the image for the purpose of modifying the actual meaning of the visual message included in it or any image manipulation becomes tampering, based upon the context in which it is used [2]. This gradual takeover of original images by the tampered images may give rise to some serious problems such as image integrity and authenticity, completeness of image, image content security etc. These tampered images have great impact on our society and pose serious threat to the security and integrity of image content.

DOI: 10.15680/IJIRCCE.2018. 0609041

The authenticity and integrity of the digital images can be achieved either by preventing it from being tampered or by detecting the tampered regions in it. There are many tampering detection techniques like Principal component Analysis (PCA), Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), Singular Value Decomposition (SVD), etc. Our research is focused on detection of tampering in digital images. This research work presents a tampering detection technique for detecting different types of tampering like copy-paste, transformation based, feature based and noise based. The proposed model is computationally less complex and is less time consuming. On the basis of literature survey, it is observed that very less exhaustive research has been carried out in this area of tampering detection.

II. LITERATURE REVIEW

A. Digital Watermarking

Digital watermarking is a technique to embed informationinto a certain image with the purpose of determining the originof the image [3]. By digital watermarking algorithm,random bits patterns, called signature, is inserted into the image[4]. The signature can be used to detect the image's copyright information, and this signature is stored within the image file itself as noise, making it difficult for detection and removal of the watermark [4]. Figure 1 shows a general block diagram of digital watermarking.

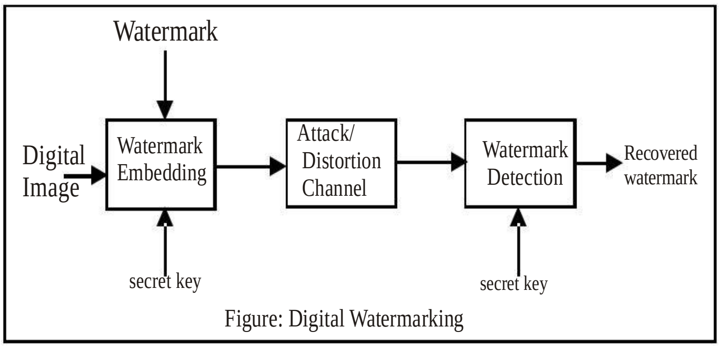

Figure: Digital Watermarking

B. Digital Watermarking Types

Watermarking has different approaches that can be used forimplementation. There are two types of digital watermarkingtechniques, which are visible watermarking and invisiblewatermarking technique.Visible watermarking is a watermarking technique thatcreates a translucent layer in front of the image, whereby thewatermarked layer overlay the image [5]. Visible watermarkingallows user to input text for the watermarking process. Thisvisible watermarking technique is used either to protect theoriginality of the image, or to make it harder for copying, forexample, money watermarks or stamp watermarks [6].However, this method is outdated in terms of security, as anyonecan eliminate visible watermark by using photo editing software,such as Adobe Photoshop. Users can edit and remove all of thewatermarked text on the image, unless the watermark fills thewhole image, which will of course impede visuals and highlyundesirable.The second method uses invisible watermarking technique.There are many types of invisible watermarking techniques. The frequency-domain technique [5] stated that this technique, which is also known asspectral watermarks, will transform the whole image into a setof frequency domain coefficients, and the watermark is thenembedded into the transformed coefficient. In this study, theDiscrete Cosine Transform (DCT) is used as the preferredfrequency-domain technique. Furthermore, the DCT method canwithstand compression and noise attack, which will be testedthrough experimentation later on.

C. Difference between Watermarking Approaches

Watermarking techniques can be compared into threeparameters, which are performance, security, and output size ofwatermarked image. Performance is calculated based on timerequired for the watermarking process to take place. If theperformance is slower, than the algorithm is not the best.However, performance has a relationship with security. If theperformance is faster, but the security is low, than the algorithmis not the best. This is also the same for the output size ofwatermarked image. The higher size of watermarked image,the lower the quality of the algorithm.

Visible watermarking is not a best way to do watermarking.It is impractical since the technology of cropping is widely used.People can crop certain area of images that are not overlaid byvisible watermark, thus creating a non-secured watermarkedimage. Nevertheless, since the speed of watermarking is fasterand the size of watermarked image is smaller than invisiblewatermarking, visible watermarking is still acceptable, but notin the form of security. Visible watermark can be used for eithermoney image or stamp image, because this kind of image isunusable if cropped. For other type of images, such as scenery,portrait, and animals, user can crop certain area of the image,and use it for certain purposes because these type of images havemany Area of Interest (AoI). AoI means a single image consists of many interesting area that can be cropped by certain users.

D. Digital Image Tampering and Detection

Image tampering defines adding or removing features from an image withoutleaving any obvious traces of tampering[6]. In terms of image processing, tampering canbe defined as changing original image information by modifying pixel values to newpreferred values so that the changes are not perceivable. This explain enhancing an image bytampering the image in order to clearly express the information content of the image shouldnot be taken as tampering. It is also called as image forgery. Digital technology has become so much advanced that even a novice of digital imageprocessing is able to create his own digital works. Availability of technology gave power ofdoing unimaginable creations in digital media, but the fact that is not much realized is loss ofcopyright protection. In 21st centuryImage tampering as piece ofart making. Companies are used tampering to retouch image to their client's preference. Tampering is normally done to cover objects in images in ordered to produce falseproof and to create the image more accurate for appearance commonly known as image retouch.The medicine reports of patients are highly confidential and are every time supposed tobe authentic.

Medical images are defines in most of the cases as proof for unhealthiness and claim of disease. Since medical images are important in dealing with huge amounts of money, people canget lured to tamper images for claiming medical insurance. Also medical reports are generally used as proofs for avoiding punishments in courts.

E. Metadata

A single JPEG image carries bundles of information that describe the image itself. This information is called metadata. Metadata is a set of data thatare embedded inside an image, includes all information that areneeded by an image that had been created, by either usingcamera or by computer.In order to increase the security and copyright of an image,metadata will be used as the embedded information inside thewatermarked image. However, a single image consist hundredsof information of the metadata. Taking all these data to embedinto an image is not advisable, as it will definitely affect thewatermarking process and results. Therefore, certain attributesof metadata that can aid in proving image originality andcopyright will be used as the embedded watermark.

III. Related work

Digital watermarking is a widely used technique to protect digital contents such as images, videos, music, etc. fromcopyright infringement, digital theft, and ownership issue.These digital contents use a very simple algorithm that can bebroken by anonymous attack. In many research areas, digitalwatermarking had been massively discussed, and manysolutions were proposed by researchers in order to increase therobustness and protection of the algorithm. [10] Proposed adigital watermarking method by implementing the combinationof discrete wavelet transform (DWT) with permutationtechnique to distort the original image and watermark, and thenbe used to embed watermark into the image. Besides that, [11]proposed the same methodology as this research, wheremetadata of image are used as watermark for the image.However, [11] used DCT integrated with BCH-protectedmetadata. Alternatively, this particular study concentrated onthe implementation of conventional visible and DCTwatermarking techniques with implementation on social mediasites. [12] Presented a hybrid combination of invisiblewatermarking technique, where frequency domainwatermarking algorithm was implemented in spatial domainwatermarking algorithm based on correlation coefficient andquadratic DCT transform. This method is proven by [12] to beeffectively robust against JPEG compression, noise, cropping,scaling, and filtering attacks.

The field of digital image processing, much work is done to detect the tampered images. The main techniques to create a forged image are basically three types but copy move is one of the easy and famous techniques. In the copy move tamper, one portion of the image is copied and moved to another part in the same image. Different methods are included to detect these types of tampered images. Recommended a technique to identify copy-move tampering, it works on analysing the image to each and every cyclic shifted version. Due to the high complexity, it become typical to implement [6].There are two methods are included; algorithmfirst works for copy-move tampering to detect the copied part (copied without any changes) at various region in same image. Second algorithm fails because it can't detect very tiny copied part and also can't handle rotated images in related work of tampering image detection. There is proposed the technique to detect the region duplication with the help of Discrete Cosine Transform (DCT). The DCT technique forgery is detected by dividing the image in the overlapping blocks and then duplicated blocks are identified. This method fails in small copied area to detect tampered blocks.

IV. PROPOSED SYSTEM

The ownership and copyright of every image can prove by metadata are as follows: Size of image, Date, Time, Path and Manufacture model. Each manufacture set path different, therefore the ways to save the image for every smart phone represent their own personality, which can prove the originality of an image. Date, Time and Model are the most important attribute in proving originality of the image. Therefore these metadata are chosen. Every smartphone's camera is capable to capture the sameimage, with different unique sizes.That is why; it can be used asadditional metadata for hardening the originality and ownershipof the image.Therefore, the proposed solution is to use metadata as the embedded information in the watermarking process.

Different types of tampering like copy-paste, transformation based, feature based and noise based are to be occurring in social media. To detect the tamper image, Proposed systemuse tampering detection technique to solve these problems.

V. EXPERIMENT DESIGN

In order to implement the algorithms of bothvisible and invisible watermarking techniques, an AndroidApplicationdeveloped. Applicationis a Javabased, used to implement and test each of thewatermarking techniques, thus constructing analysis based onthe results of output images, watermarked using this application.Within this experiment, three parameters are tested andanalyzed on both watermarking techniques. These parametersare; performance measurement, security measurement, andupload and download results and affect on the watermarkedimages to social media.The performances of these watermarking techniques areseparated into two sub-parameters, which are the completiontime of the watermarking process, and the size of thewatermarked image. Both sub-parameters are measured, and theresult is analyzed, by comparing the size of original images tothe watermarked images, and the time taken for eachwatermarking processes to complete for both watermarkingtechniques is noted.The security of each watermarking techniques is analyzed bymeasuring the robustness of each watermarked images to bypassimage cropping and print screen attacks. If the embeddedmetadata in all of the watermarked images preserved during theattack, then the technique is considered secure. For croppingattack, each of the images will be cropped randomly, based onthe AoI for each image. Print screen attack is done by printscreening the whole image, and then testing it for the presenceof embedded watermark. If any watermarked images of thewatermarking algorithms can passed through both attacks, thenthe algorithm is robust enough to withstand both attacks.

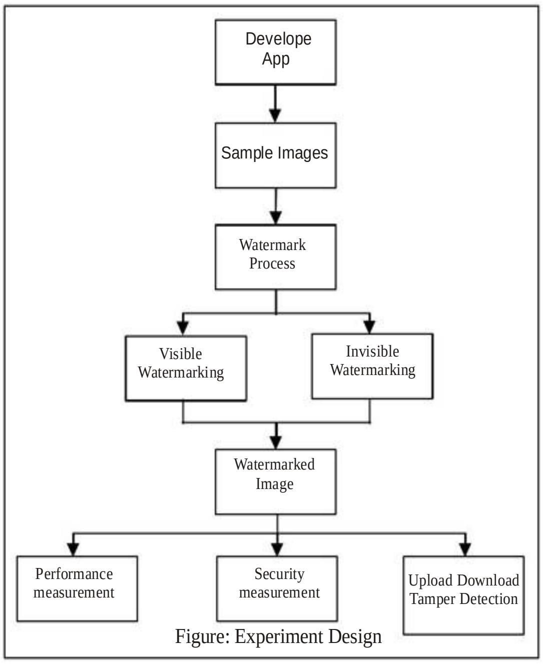

Figure: Experiment Design

This aims to investigate whether the embeddedmetadata inside watermarked image can successfully passthrough the uploading process without being detected anddeleted by the social media sites. In order to archive this aim,each of the watermarked images will go through uploadingprocess into four different social media sites, and the images willbe downloaded back for analysis purposes. It is to observe whether embedded metadata inside the watermarked image ispreserved during the uploading and downloading processes.The overall experiment design is compressed and illustrated in Figure.

VI. APPLICATIONS

Digital Watermarks are useful invarious applications; the focus of each application is to providing security of the digital contents including:

- **Ownership:** To prove ownership assertion watermark can be used. Using secret private key which can be embedded into the original image for providing ownership assertion.
- **Fingerprinting:** Multimedia content is electronically distributed over a network applications, the owner would like to discourage unauthorized duplication or duplication by embedding a watermark (or a fingerprint) in each copy of the data. If, after unauthorized copies of the data are found, then the origin of the copy can be found by retrieving the fingerprint. Therefore application needs to provide invisible watermark and must also be invulnerable to deliberate attempts to forge, remove or invalidate.
- **Copy prevention:** For copy prevention and control Watermarks can also be used. Copy of image each time is made the watermark can be modified by the hardware. Example of such a system is the DVD. In fact, a copy protection mechanism that includes digital Fraud and tamper detection.
- **ID card security:** The photo that appears on the ID or Information in a passport. ID card verified by using extracted embedded information. Additional level of security provide by using watermark in this application.
- **Fraud and Tamper detection:** If multimedia content is used for legal purposes, medical applications, reporting, and commercial transactions, it was originated from a specific source and that it had not been changed, edited or manipulated. By embedding a watermark in the data it will decrease the fraud. When the image is checked, the watermark is extracted using a unique key embedded with the source, and the integrity of the data is through the integrity of the extracted watermark. Watermark can include detail information from the original image that can help in undoing any manipulation and recovering the original image. Watermark used for authentication purposes should not damage the quality of an image and should be secure the image.

VII. CONCLUSION AND FUTURE WORK

The simulation results showed that usage of metadata embedded into images before uploaded into social media to better secure ownership, decrease unauthorized sharing of images andreduced identity fraud. The proposed system provides image tampering detection by using efficient algorithm and also checks the changes in metadata which is embedded in image after the uploading on different social media sites.The experiments shown that it is difficult to be employed in social media, where ownership details or information are stripped away or tarnished from uploaded images in their sites.

The performance of the digital watermarking methods designed, developed and tested in this paper are evaluated against compression attacks only, so this can be extended to other image processing attacks like cropping , scaling and rotating. These techniques are not tested for video watermarking. Conclusively, social media users are urged to be more careful in what they share online, or use a different service to keep privacy.

REFERENCES

1. N. Srivadana , “DIGITAL WATERMARKING”, International Journal for Technological research in Engineering ,Vol.1,Issue 3, pp. 2347-4718, 2013.
2. Hong-ryeol Gil1, Joon Yoo1 and Jong-won Lee2,’An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks’, Proceedings of the 2nd International Conference on Human. Society and Internet HSI'03, pp. 302-311,2003.
3. Heather Wood (2007). Invisible Digital Watermarking in the Spatial andDCT Domains for Color Images. Adams State College, Alamosa,Colorado.
4. Mazleena Salleh, Subariah Ibrahim and Ismail Fauzi Isnin (2003). Image Encryption Algorithm based on Chaotic Mapping. Jurnal Teknologi. 39(D), 1 – 12.
5. Namita Chandrakar and Jaspal Bagga (2013). Performance Comparison of Digital Image Watermarking Techniques: A Survey. International Journal of Computer Applications Technology and Research. 2 (2), 126 – 130.

6. J. Fridrich, D. Soukal, and J. Lukas, “Detection of Copy-Move Forgery in Digital Images”, in Proceedings of Digital Forensic Research Workshop, August 2003.
7. Statista (2016). Statistics and facts about Social Networks. Statista Retrieved March 19, 2016, from http://www.statista.com/topics/1164/.
8. Oxford University Press (2017). Definition of social media in English. English Oxford Living Dictionaries. Retrieved April 13, 2017, from https://en.oxforddictionaries.com/definition/social_media.
9. Nobuo Ezaki, Marius Bulacu Lambert , Schomaker , “Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons” , Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, pp. 683-686, vol. II, 2004
10. Hsiang-Cheh Huang, Wai-Chi Fang (2010). Metadata-based Image Watermarking for Copyright Protection. Simulation Modeling Practice and Theory, Vol. 18, Issue 4, pg 436-445.
11. Md. Selim Reza, Mohammed Shafiul Alam Khan, Md. Golam Rbiul Alam, 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.
12. TSR Watermark Image. (2016, April 1). Retrieved April 1, 2016, from http://www,watermark-image.com/watermarking.aspx/