ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Image Security in Social Media using Digital Watermarking with Embedded Metadata

Mr. Bilal Sayyad [1], Mr. Mubarak Sache [2], Mr. Vaseemakram Sayyed [3], Prof. Deokate V.[4]

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

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

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

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

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. 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. RELATED WORK

Digital watermarking is a widely used technique to protect digital contents such as images, videos, music, etc. from copyright infringement, digital theft, and ownership issue. These digital contents use a very simple algorithm that can be broken by anonymous attack. In many research areas, digital watermarking had been massively discussed, and many solutions were proposed by researchers in order to increase the robustness and protection of the algorithm. [10] Proposed a digital watermarking method by implementing the combination of discrete wavelet transform (DWT) with permutation technique to distort the original image and watermark, and then be used to embed watermark into the image. Besides that, [11] proposed the same methodology as this research, where metadata of image are used as watermark for the image. However, [11] used DCT integrated with BCH-protected metadata. Alternatively, this particular study concentrated on the implementation of conventional visible and DCT watermarking techniques with implementation on social media sites. [12] Presented a hybrid combination of invisible watermarking technique, where frequency domain watermarking algorithm was implemented in spatial domain watermarking algorithm based on correlation coefficient and quadratic DCT transform. This method is proven by [12] to be effectively 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; algorithm first 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.

III. 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 smart phone's camera is capable to capture the same image, with different unique sizes. That is why; it can be used as additional metadata for hardening the originality and ownership of 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 system use tampering detection technique to solve these problems.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

IV. RESULT AND ANALYSIS

Based on the developed application, experimenting phases for each watermarking techniques had been conducted. The experiments were based on the experiment design explained on the previous section, which are performance measurement, security measurement, and upload download test. The results were analysed based on the degree of this research.

A. Metadata Analysis

Based on the data captured, the sequence of metadata retrieved by each devices are slightly different. A sequential technique for implementing metadata towards image watermarking is not practical. Therefore, a meaningful metadata must be selected, that can prove ownership and copyright.

Manufacturer and model	1	2	3	4	5
SAMSUNG Galaxy Note 3 Neo	Model	ISO	Brightness	Aperture	Shutter speed
XIAOMI Redmi Note 3	Date	Title	Size	Resolution	Model
HUAWEIP9 Plus	Title	ISO	Shutter speed	Exposure	Focallength
OPPO Neo 7	Title	Time	Width	Height	Orientation
LENOVO Vibe Shot	Title	Time	width	Height	Orientation
HONOUR 4C	Title	Model	Time	Size	width

Table 1: Analysis of Metadata in different Devices

Five selected metadata:

- Manufacturer: Provide exacts smart phone's manufacturer.
- Model: Show the smart phone's model.
- Path: Display the path where the image had been saved.
- Size: Show the actual size of the image (either in KB or B).
- Time: Display time and date the photo had been taken.

B. Performance Measurement

Using different images experiment conducted watermarking process for algorithm. Based on size of image performance will measured and completion time also. Below Table dhow the results for these experiment.

Watermark	Compare Watermarked image with original image	Average difference
Visible	Larger	68%
DCT	Smaller	24%

Table 2: Watermarked Difference between and Original Image

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Result show that the visible watermarked images larger than the original images with 68% difference and 24% difference for DCT Watermarked images. Above result cannot be determine the effective algorithm therefore second parameter is to calculate average time taken to complete watermarking process is to be measured. Below table show the average time taken to complete the watermarking process.

Watermark	Average Time Taken to Complete Watermarking Process(seconds)
Visible	1.4 seconds
DCT	23.2 seconds

Table 3: Average Time Taken to Complete Watermarking Process

The result shows that the visible watermarking process is faster than the DCT watermarking process. Visible watermarking process completed in 1.4 seconds which is faster than DCT. DCT watermarking process required 23.2 seconds to complete the process. Visible watermarking techniques take a shorter time because there are no complex calculations involved in processing watermarked images. Invisible watermarking, however, uses a very complex calculation, with some pixels separation, making processing time a bit longer.

Visible watermarking is faster compared to DCT watermarking, it does produce large image which is affects on efficiency. The DCT technique is slower due to its processing needs. This is because the image had been recalculated, rescaled and reconstructed back after watermarking process is done.

C. Security Measurement

By applying cropping and print-screen attacks on image to test the security of an image. These attacks are used to test the robustness of algorithm which we used in above experiment. Below is the result of the experiment:

Watermark	Cropping attack	Print-screen attack
Visible	Success, watermarked text disappeared	Failed, watermarked text preserved
DCT	Success, watermarked disappeared	Success, watermarked disappeared

Table 4: Attacks done towards watermarked images

The print-screen process will print the visible watermarks as well, although this can be easily cropped out later. With the DCT watermarking process however, the embedded watermark cannot be detected anymore. Cropping any AoI, avoiding the watermarked region can be easily done. The DCT watermarking technique also failed to evade this attack.

D. Upload & Download Process for Watermarked Images

To test the process of uploading image on social media on four different sites as shown in below table. The watermarked images for both visible and invisible watermark were uploaded into four different social media sites. These images were then downloaded back to test the presence of embedded watermark. Below are the result of this experiment:

Social Media	Visible Watermark	DCT Watermark
Facebook	Pass	Pass
Whatsapp	Pass	Pass
Twitter	Pass	Pass
Instagram	Pass	Pass

Table 5: Presence of embedded watermark

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Based on result shown, all visible watermarked images passed the experiment. It is because it only change the size, resolution and quality of image. The embedded metadata of the image are preserved. For invisible watermark the image is successfully uploaded and extracted the embedded metadata.

V. CONCLUSION AND FUTURE WORK

The simulation results showed that usage of metadata embedded into images before uploading into social media to better secure ownership, decrease unauthorized sharing of images and reduced 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. Thus we concluded that all the parameters are worked successfully. The embedded metadata into the image extract successfully and uploaded the image on social media to providing the security.

Hence we have successfully implemented the android application which provide digital watermarking to image for security purpose on social media. 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 and DCT 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/