ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

DAC for Mobile images using Watermarking technique with Cloud Computing support

S. Deepika, Assistant Professor, Computer Science and Engineering, Kings Engineering College.
M. BalaEswari and P. Jeyanthi Priya, Computer Science and Engineering, Kings Engineering College

***Abstract*—The millions of active users all around the world are using online social network, such as Facebook, Twitter and Tumblr and LinkedIn. The majorities of social networks have weak user to user authentication method, which is based on some basic information like displayed name, photo. These weakness make it effortless to misuse user's information and do identify cloning attack to from fake profile. In this proposed system, watermarking technique is used to hide the copyright information in the uploaded pictures and requires admin permission to download the document even though downloaded by the registered user. The Discrete Wavelet Transform Technique is used for transferring and embedding the watermark to the image where the java static watermarking systems and algorithms is been used as watermarking technique. Any fake users updating the same data can be detected and their respective MAC address would be tracked and blocked.**

***Index Terms*—Discrete Wavelet Transform, MAC address, Watermark embedding, Watermark extraction.**

I. INTRODUCTION

THECloud Computing is the ability to access a pool of computing resources owned and maintained by a third party via the internet. With the advent of Cloud Computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data [1]. Nowadays, people are recording their daily lives and share their pictures in social media as public and private data. People can easily upload their images or other multimedia content, which can be easily accessed and downloaded by others [2]. Simplicity of downloading the data from the network seems to encourage people to use the data without authorization. Unauthorized use of data can be a form of copyright violation. It is common on the World Wide Web (www) for the maximum data to get copied from one site to the other without the consent of the original data developer [5].

In most cases, users do not retain the copyright of the uploaded images and, accordingly there is no way to certify the ownership of the digital content. To avoid this kind of situations, efficient and robustness techniques are required for digital image copyright protection and authentication [10]. Digital image watermarking provides copy right protection to the image by hiding appropriate information in original image to declare the rightful ownership.

The rest of this paper is organized as follows. Section II Reviews related work in Multimedia. Section III presents the Existing systems and solutions. Section IV presents the proposed system of this project. Section V depicts the detailed analysis of system design. Section VI presents the algorithm of watermarking. Finally, we conclude this paper with future enhancement in section VII and conclusion in Section VIII.

II. RELATEDWORK

It has become a daily need to create copy, transmit and distribute the images as a part of widespread multimedia technology in internet era [8]. The majorities of social networks have weak user to user authentication method, which is based on some basic information like displayed name, photo.Hence copyright protection has become essential to avoid unauthorized replication problem.

A. Watermarking

Watermarking is the process of hiding digital information in a carrier signal. Digital watermarking is a technique to protect host digital data by embedding the data properly like the company logo or image, copyright information into the data. Watermarking has been around for several centuries, in the form of watermarks found initially in plane paper and subsequently in paper bills [12]. However, the field of digital watermarking was only developed during the last 18 years and it is now being used for many different applications. Watermarking technique can be classified into various types based on four categories such as working domain, type of documents, human perception and application.

According to working domain, the watermarking technique can be divided into two types such as spatial domain and frequency domain. According to type of documents, the watermarking technique can be divided into four types such as text, image, audio and video. According to human perception, the watermarking technique can be classified into two types such as visible and invisible. Visible watermarking can be divided further into two types as robust and fragile. According to application, the watermarking technique can be divided into two types such as source based and destination based [10].

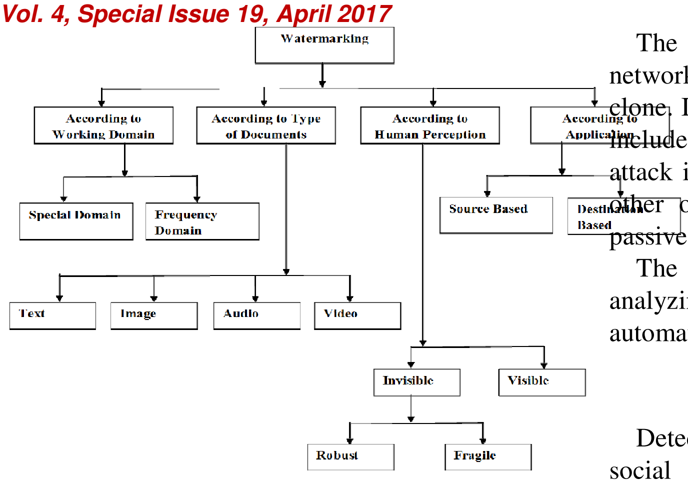


Figure: Types of watermarking techniques

B. *Frequency Domain*

The watermark is embedded in the spectral coefficient of the image, in frequency domainwatermarking technique. The characteristics of the human visual system (HVS) are captured more effectively by the spectral coefficients so the watermarking in frequency domain is widely applied. The common algorithms used in frequency domain are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). [3] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation.

In DCT data is represented in terms of frequency space rather than an amplitude space. When compared to spatial domain watermarking technique based on DCT is more robust [2]. These algorithms are robust against digital image processing operations like low pass filtering, brightness and contrast adjustment etc. These are computationally more expensive and difficult to implement.

DWT is a modern technique, widely used in digital signal processing, image compression and watermarking etc. These transforms are based on small waves, called wavelet, of varying frequency and limited duration [2]. The wavelet filters are used in this technique to transform the image.

III. Existing Solution

With the broad distribution of On-line Social Networks, the privacy and confidentiality of the users involved in such services is going to be a key distress.The possibility of mounting threat attacks on identity on online social network with two alternatives: single-site online social network and cross-sites online social networks.

The victim encompasses a profile in the online social network where the attacker would form the profile which is clone. In cross-site online social networks, the victim does not include a profile in the similar online social network where the attack is run; however, the profile of the victim is present in other online social networks. Clone attacks are of active, passive and semi-passive.

The existing systems such as traffic analyzing and graph analyzing methods are all human monitoring method and not automatic.

IV. Proposed System

Detection and identifying the fake profiles and botnets in social networks are restricted to user’s report and just subsequent to a number of reports for particular user; the system will check the validation of user.

In the proposed approach, watermarking techniques and methods will be used to detect and identify such fake profiles. In this method, at any time a user uploads his/her pictures, some exclusive and useful information such as email or username and also date of upload would be attached to pictures by means of watermarking methods. Accordingly, in future, if somebody else saves that picture and attempts to create a fake profile with stolen data, the system is able to automatically detect this deception and fraud and would prevent and protect the fake user from any additional positive action.

Our proposed system invokes discrete wavelet transform algorithm for data hiding. Thus this would prevent the clone attacks and providing complete user data privacy preserving. Also when users upload the profile picture or photos it would be watermarked and updated. For watermarking technique Java static watermarking systems and algorithms is been used. Any fake users updating the same profile picture can be detected by sending the notification to the owner and their respective IP would be tracked and blocked according to the owner decision. Also in our project to provide secure authentication we have invoked certain attributes which can be asked to the users during registration. Thus we can able to avoid clone attacks in social media networks.

V. System Design

Main aim of the project is to provide copyright protection to images over the web. Generally our web site is probably the product of hundreds or thousands of hours of work and an investment of thousands of dollars. Butany or all of our original content could be easily copied and displayed by the third-party or unauthorized user. To overcome this type of problem copyright protection is needed.

Watermark is a message which is embedded into digital content (audio, video, images or text) that can be detected or extracted later for copyright identification. Such messages mostly carry copyright information of the content author.

Watermarking has been revealed to be an efficient technique to cope with the problem of intellectual property rights (IPR) protection of multimedia data [11]. This technology embeds into the data an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected.

We mainly concentrate on download and upload of images safely through watermarking in the social network where the authenticated user only can download or upload the images only with the admin user (image author) permission. The image is watermarked when it is initially uploaded to the network itself.Thisimage is watermarked by the information of the author who is uploading the image initially to the cloud and it is stored in the server.

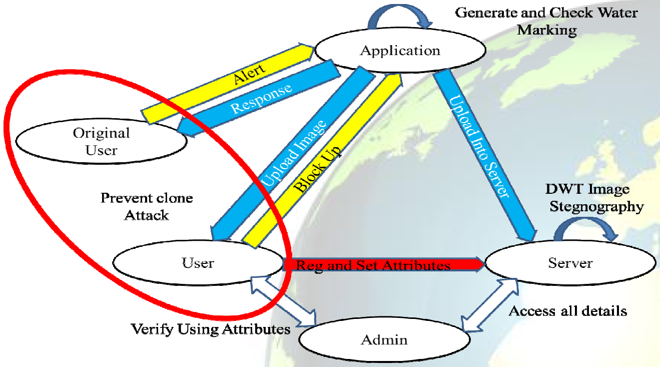


Figure: System Architecture

A. Social Network

Online social network presents a wide variety of online uses that exhibit a series of challenges to the security. The security and privacy threats increase, as the amount of personal information posted by users in their profile is made public. Majorities of social networks have weak user authentication method, which is based on some basic information like displayed name, photo. These weaknesses make it effortless to misuse user's information and do identity cloning attack to form fake profile [6]. We use data hiding techniques to hide some information in profile pictures in order to detect botnets and fake profiles and finally will propose an automated model to detect fake profiles and botnets instead of current manual method.

B. Static Watermarking

A Static Watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal [10].In this method, at any time a user uploads his/her pictures, some exclusive and useful information such as email or username and also date of upload would be attached to pictures by means of watermarking methods.

If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied pictures or media. This watermarking scheme is widely utilized for authentication of data, copyright protection and communication process. Watermarking generally consists of two phases; watermark embedding i.e. introduce smallimages or pattern into the data without affecting the original data [10]. A key is used to embed the watermarkinformation into the data; once the watermark information is embedded the data is available for the use. Anotherphase is watermark detection or verification this phase is used to verify the ownership of the data. The data iscompared with the suspicious database using the same key.

C. Image Steganography

Information hiding techniques are broadly classified into four categories such as Covert channels, Steganography, Anonymity and Copyright making. Steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography is a technique of hiding an encrypted message so that no one suspects it exists [9]. Ideally, anyone scanning your data will fail to know it contains encrypted data. The discrete wavelet transform is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules.

We use discrete wavelet transform algorithm for data hiding. Thus this would prevent the clone attacks and providing complete user data privacy preserving. Also when users upload the profile picture or photos it would be watermarked and updated. The steganography procedures can be technical were as the copyright making procedures can be robust.

D. Intrusion Detection

An intrusion detection system (IDS) is a software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

In this method, system will automatically check the right and privilege of the user and ownership of uploaded file. Subsequently to checking the uploaded file, if the system finds the existence of watermark, it will send an announcement and a notification to the owner of original content and prevent User from re-uploading.

E. Alert and Block

.If the system finds the existence of watermark, it will send an announcement and a notification to the owner of original content and prevent User from re-uploading. Fake users updating the same profile picture can be detected and their respective IP would be tracked and blocked.

VI. Algorithms and Techniques

A) Watermarking Algorithm

Lot of research is going on in the field of watermarking because watermarking is not a fully matured technique.Watermark embedding i.e. introduce smallimages or pattern into the data without affecting the original data.

Input: Original Image.
Output: Watermarked Image.
Algorithm:

```
Step1: Read the Input Image.
Step2: Receive the rendering graphics property of the input image.
Step3:Create buffered Image Object of same width and height as of the input image.
Step4: Decompose the source image into grayscale image.
Step5: Read the graphics properties of the source image.
Step6:Select and set the watermark text.
Step7: Set the font and color for the watermark text selected.
Step8: Calculate the coordinates where the text string is to be painted.
 X = (sourceImage.getWidth () - (int)rect.getWidth ()/2.
 Y = sourceImage.getHeight ()/2.
Step9: Paint the textual watermark on the input image.
Step10:Write the watermarked image.
```

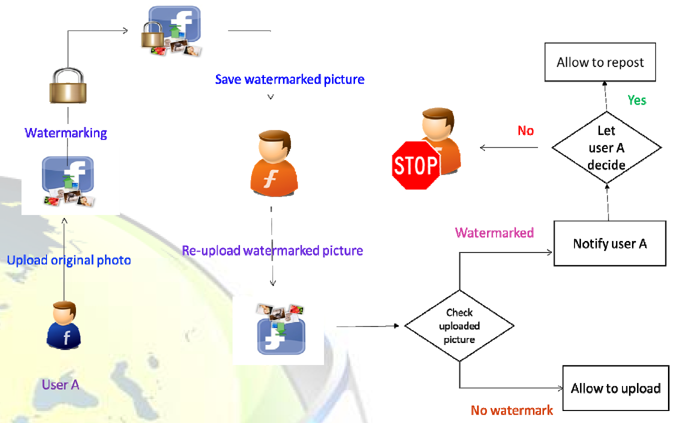
The java static watermarking is a visible watermarking technique in which the watermarked text is visible without disturbing the image visual property more. Static watermarks are stored in the application executable itself [12]. For example this could be stored in the initialized data portion of the executable resources. If an image has to be watermarked then the graphics properties of that image has to be read initially. The following two figures represent an image before watermarking and after watermarking.

(A)Before Watermarking

(B) After Watermarking

B)Allow and Block Technique

An image is watermarked for copyright protection of it. But the author of the image who is the owner has to be notified if anyone is misusing the image[1]. For this in our project we introduce allow and block technique where the owner of the image is requested mandatorily to give permission for the user to download or upload the image in the cloud. This is achieved by comparing the byte stream of that image with the original image in the cloud. If any changes in comparison are found, then the owner for the image is found by searching it in the database. Then a notification to that owner is send with allow and block option for that image for that concerned user. If the owner of the image allows the user then that user can download or upload the image. If the owner of the image blocks the user then that user is blocked to download or upload that image. When an image is uploaded to the cloud, first it is checked for the availability of watermarking. If there is no watermarking in that image then the cloud considers that user who is uploading that image as its owner. Therefore allow and block technique is called only when the watermarking is found in the uploading image. The following is the flowchart for the allow and block technique



VII. Future Enhancement

In future, the project can be enhanced by improving the watermarking algorithm with the combination of both visible and invisible watermarking which will not be disturbed by the noises. Furthermore researcheshave to be done for the new algorithm from the combination of visible and invisible watermarking.

VIII. Conclusion

One of the major challenges in the Cloud Computing is security. In last few years, Digital watermarks have thus helped us to protect the ownership of digital data. The Copyright Protection of web applications through Watermarkingby us has made the best possible efforts to satisfy the needs of Users. Digital watermarking scheme is widely utilized for authentication of data, copyright protection and communication process. It provides a consistent robust performance on different original image and watermarked image in various analyses. The details of the user are registered and then the user is requested to enter the image to be watermarked. Then the watermark creation and embedding can be done based on blind watermarking with in a very less time, based on the key.The user can check the image whether he got the correct one or not. Thus the copyright protection and security for the images against clone attack in the cloud can be provided by this method.

REFERENCES

Basic format for books:

[1] H.Yue, X. Sun, J.Yang, and F.Wu, "Cloud-based image coding for mobile devices-toward thousands to one compression," IEEE Trans. Multimedia, vol. 15, no. 4, pp. 845–857, Jun. 2013.

[2] Nielsen, Social Networks and Blogs, 4th Most Popular Online Activity, Nielsen Online Report, 2009..

[3] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[4] Stolen Facebook Accounts for Sale, http://tinyurl.com/25cngas,2010.

[5] Personal communication with the Manager of User Support and the Product Manager of the Core and Community Management teams in Tuenti, 2011.

[6] Fake Accounts in Facebook - How to Counter it, http://tinyurl.com/5w6un9u, 2010.

[7] Why the Number of People Creating Fake Accounts and Using Second Identity on Facebook are Increasing, http://tinyurl.com/3uwq75x, 2010.

[8] Jun Wu, "Dac-mobi with Cloud Computing support", *IEEE Trans. Multimedia,* vol. 18, NO. 5, May 2016.

[9] James Hays and Alexei A. Efros, Carnegie Mellon University, "Scene Completion using Millions of Photographs", Computer Graphics Proceeding, Annual Conference Series, 2007.

[10] Mrs.Anitha.P and Dr.Malini M Patil, Department of Information Science and Engineering, *JSSATE(India),* "A survey on watermarking methods for security of cloud Data", IJARSE, Vol. No.5, Special Issue No.(01), Feb 2016.