

Digital Image Identification over Social Network

Neeraj
Bhargava, , Ph.D
Dept of Computer
Science, School of
Engineering & System
Sciences.
MDS University
Ajmer,Rajasthan

Ritu Bhargava, Ph.D
Department of MCA,
Government Women's
Engineering College
Ajmer,
Rajasthan

Manish Mathuria
Department of C.S. &
I.T.,Govt. Engineering
College Ajmer,
Rajasthan

Minaxi Cotia
Dept of Computer
Science, School of
Engineering & System
Sciences
MDS University
Ajmer, Rajasthan

Abstract

Internet is the base of web based communication. The electronic transfer is only possible when both the parties recognize each other. In other words, only authorize parties can make electronic (money) transfer over the Internet; the security is the main concern here. Social Networking is a basic need of the generation, today. Users share their private information in the form of text or media like: Image, Audio and Video over the Social Networking websites. The main drawback of social networking is: faker can easily create fake accounts by representing personal information (like name and profile picture) of others, because it is easy to copy from the browser directly. Now, the question arises: "What is the Unique Digital Identity of user over the Social Network?" This research paper discusses about the security concerns over Social Network. The researched analysis provides a solution to the problems regarding privacy of a Digital Identity by using Digital Watermarking, where Digital Fingerprint Image is use as Watermark to embed with Profile Image using DWT.

Keywords

Digital Identity; Social Identity; Social Network;
Digital Watermarking; Digital Fingerprint Watermarking;
Color Image, Digital Watermarking

1. INTRODUCTION

It is an era of Digital Information Technology known by Digital World. Since 2000, the dependence of human on the computers is increasing. The development of new technologies focuses on the availability of digital information to the audience. As the concept of Open Source, is being acceptable by innovators of Information Technology, the demand of digital information (or data) is also raising.

The Open Source concept provides freedom to individuals to change according to their requirement, but it is also a drawback which gives access to fakers to illegal use to freedom.

As a Citizen of a Country, if one can get a Unique Identification by Unique ID (or UID) Card, then: "Why not on Social Networking?" Because, Social Networking is a part of life where one can freely share their thoughts with their known.

It is main objective of this research paper to provide general awareness about the importance of Digital Identity on the Social Network. [1]

2. DIGITAL IDENTITY VERSUS SOCIAL IDENTITY

2.1 Digital Identity

It is the identity of Digital Data which reflect to the owner. Basically, data on computer or mobile devices can only be share digitally via network, so the owner of digital content define by some digital information known as Digital Identity. The Digital Identity over the digital network is specified by the location of existence and activity associated with the user over the network. [2]

2.2 Social Identity

The Social Identity is the identification of any entity at Social Network. The Social Network either digital or human is an association which itself provides a communication medium. People respective to their communities require an Identity (or designation) to present something to their followers known as Social Identity. And the activity of any member associated to their Social Network is known as Social Networking. The member of a social network can socially collaborate on an event to their community by reflecting their Social Identity. [3]

2.3 Concluded Points of Discussion

- The Digital Identity only use to reflect digital presence activity of an entity, it does not associate personal information of individual user.
- Whereas, the Social Identity not only associates the personal information but it also contain Social relationship information.
- In both the cases, user got the identity to present something, but there is no system to prove the identity of the user.
- By incorporating features of both (i.e. Digital Identity &

Social Identity), the new term can be deduce is „Digital Social Identity“. It is the key concept of this research as the objective is to present major problems of Social Networking Users with their privacy.

3. SOCIAL NETWORK

The working principle of Social Network is to provide a social platform for everybody to share their thought by expressing through media. It follows the Open Source concept by allowing users to use application and share their data without and cost or subscription. The common functionalities provided by any Social Networking website are:

Finally, complete content and organizational editing before formatting. Please take note of the following items when proof reading spelling and grammar:

3.1 Groupware

It is the fundamental of any Social Network which creates Networks of Network. Basically, a Social Network, itself is a collection of many individual networks. These networks are created by a tool or an application known as Groupware. In other words, Groupware is used to create groups as well as manage them. There are two types of Groupware:

3.1.1 Unprotected Groupware

It is the old concept of creating a groups and then inviting people to join the group. This type of Group facilitate of share content but does limit it to users i.e. the shared content is visible to all the user connected.

3.1.2 Protected Groupware

It is the advance Groupware which facilitates to create individual groups and restrict the accessibility to individuals. This type of Groupware provides advance sharing features by assigning privilege to the content, but still it require some laws of policies that must be place to provide safeguards and assurance.

3.2 Active Wall (or Sharing Wall)

The social networking websites provides a platform to individual user so that user may express their thoughts with their followers (or Connected People). The advance social networking sites help user to explore their digital content like web-pages, images, audio files and video files. The Sharing Wall is a medium of communication to the members of group. The Active Wall actually, reflects the overall activity of any user belonging to it over the Social Network.

3.3 Like and Comment

The people over the social network can express their opinions to the shared data through two operations: First, they can like or dislike the digital content by pressing counter button (which counts the number of likes and dislikes). Second, they can write their views as comments on the textboxes available with shared content. The secure sharing restricts the commenting from unwanted users.

3.4 Cloud Storage (or User Space)

The Digital Social Network is a common platform to share the information over the internet. The internet itself includes multiple servers. The servers over the internet share their resources like storage, computation known as Cloud System. The primary use of Cloud System or Computing is to avail common place for data storage. The Social Network is implemented on this basic principle of Cloud Computing. It provides Cloud Storage and an interface to interact with. By using social network user can view, edit, download, and delete their personal data anytime, anywhere.

3.5 Chatting and Messaging

Text based communication initiated with the chatting application. Actually, the Chatting accomplish by identifying the IP addresses at both the ends and then communicating IP to IP. It is a real-time communication. Earlier, there was no intermediate system to store messages during the chat. It was only user oriented; the user himself stored the chatting history to the separate file.

Now, social network provides advance Chatting which is actually incorporated with the message functionality. Every user got their personal identification as User ID. This ID can only identify the existence to user over the Social Network. So, chatting may perform between the users by their ID to ID, it is called dynamic conversion. Alternatively, users can create messages to other by just expressing their User ID's, it is called static conversion. The advance social networking combines both the principles on common place. Now, dynamic chat may also stores as messages.

3.6 Video Calling

This feature makes a social network to the complete communication tool. Without the option of Video Calling users might move to other tools. In that, they need to create other account to use the services. But the most popular social networking sites itself provide a Video Calling tool. It is the big advantage of social networking to provide a single platform for communication to their known.

4. SECURITY ISSUES OVER SOCIAL NETWORKING

Security is the basic requirement of any transaction over the Internet. The core concept behind the security is the authentication using Username and Password. It is the basic authentication, but sometime one needs special authentication system especially over the Digital Social Network. Before going to discuss about security issues over the Social Networking, one need understand "What is the importance Digital Identity?" [3]

4.1 What is the Importance of Digital Social Identity?

As discussed above, the Social Identity over Social Networking websites is defined by Digital Social Identity. It is the combination of both digital identity and social identity. Once any user creates an account on social networking website, the website asks about some personal information's as name, email, phone number, location (address), etc while this information is mandatory to create account. It is fine when someone shares their personal information with social networking site to create an account, but „what is the surety?“ that the information will not be share to others. And if anyone can see one's personal information then it is not unique, anyone can create an account using other's personal information over the internet. It is a very big problem considering personal uniqueness of any user over the social network. It is the correct time, when IT industry needs to be focus on the Digital Social Identity. The one solution to the problem is to find out one factor as personal information that can present the personal uniqueness to the user and that should not be shareable. This research provides a solution to the Digital Social Identity by hiding Digital Fingerprint with personal information. [3] [4] [5]

4.2 Security Issues

- Anyone can create fake account.
- Fakers can pretend as original user, by just using otherspersonal information and image. No one can blame on anybody.
- If someone wants to block their fake accounts, there is no one to listen.
- If any private document or image is copied by others and they use as their own document or image. Then, original user has nothing to prove.
- If user shares their personal photographs only with connected friends. And if connected friends share it with their own friends. Then sometimes unknown people got access to the personal data of others. [6]

5. DIGITAL SECURITY TECHNIQUES

Authentication is a process which is used to identify an identity. The Digital Authentication involves the identification process to identify the source of information. Digital Authentication in the terms of digital data communication has two popular techniques:

5.1 Digital Signature

It is just digital information (signature) which privately authenticates the sender of information. The encryption is used to sign message with a private key at sender. And at the other end i.e. receiver can verify the signature by using sender's public key.

5.2 Digital Certificate

A separate digital file of information to be attach to the server which identify the certified existence of the server. Whenever, an entity wants to share information from the server-computer, it will first ask to the server for certificate. The server will issue a certificate, and then entity will verify the certificate. If verification is success, the entity can share information with server without any danger.

The Digital Authentication System is the basic requirement, so new laws must be place to provide safeguards and assurance.

5.3 Digital Watermarking

Watermark is very old technology which is prominently used for tracing copyright infringements and for banknote authentication. But now, one can use digital watermarking technique to mark the digital signal such as audio, picture, video, texts or 3D models. Definition of Digital Watermarking:

“Digital Watermarking is a technique which is used to mark some information inside the digital media for ownership identification.”

Or

“Digital Watermarking is a technique to hide owner data inside the digital media for copyright protection.”

Basically, Watermark itself is a digital identity which holds user's identical information. The Digital Watermark may further used to verify the authenticity or integrity of the media. The principle of Digital Watermarking allows to impressing information but does not allow degrading quality of data.

Fingerprint as Watermark

It is the basic approach of this research is to use fingerprint image as a watermark. The fingerprint is itself is used to uniquely identify the person. So, one can use Digital Fingerprint Image as Watermark.

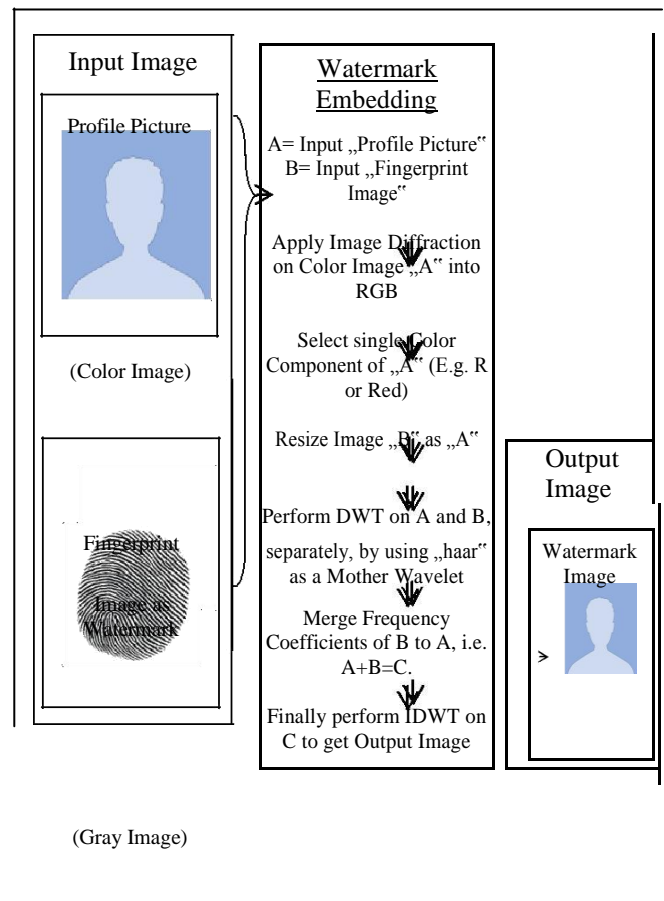


Fig. 1. Block Diagram of Color Image Digital Watermarking selecting Fingerprint Image as Watermark.

As discussed above, digital fingerprint is the important factor which can only be used to identify the personal identity, but it should be invisible. The invisible watermarking is achieved by DWT i.e. Discrete Wavelet Transform.

Figure1, is a block diagram of basic approach to use fingerprint as watermark. The middle block named as „Watermark Embedding“ expresses the algorithm and their steps to embed Watermark inside the Color Image using DWT (Discrete Wavelet Transform), where IDWT (Inverse Discrete Wavelet Transform) is used to recreate Profile Image from frequency coefficients [7]. The two dimensional Discrete Fourier or Cosine Transform are represents their forward discrete transform function as $F[u,v]$ which is entirely a function of the spatial frequency u or v . There is no direct information about the pixel or spatial variable. Similarly, Discrete Wavelet Transform uses other kind of basic functions i.e. Haar, Daubechies, etc. These basic functions are also known as Mother Wavelet. In this research, Haar is used as Mother Wavelet. [8][9]

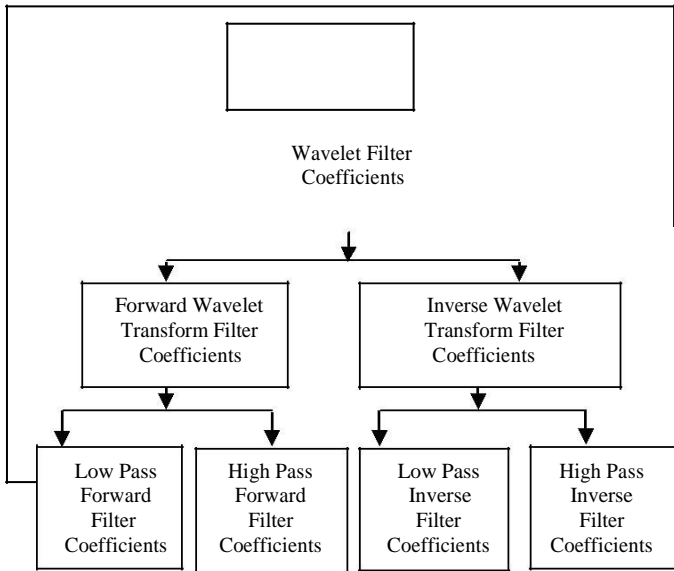


Fig. 2. Wavelet Composition of High and Low filters [9].

6. EXPERIMENT AND RESULTS

6.1 Selection of Profile Picture as Input Image

User has freedom to use any image as a profile picture. The experiment is performed on a sample image named "Flower.jpg". It is a color image and the watermarking performed is known as color Image Digital Watermarking.



Fig. 3 Input Image: Flower.jpg

6.2 Selection of Fingerprint Image as Watermark



Fig.4 Fingerprint Image: Fiingerprint.jpg

Watermarked Profile Picture



Fig. 5 Watermarked Image: W_Flower.jpg

6.3 Recovered Watermark from the Watermarked Profile



Fig. 6 Recovered Watermark Image: RW_fingerprint.jpg

TABLE I. IMAGE QUALITY TESTING

Image Type	Peak Signal to Noise Ratio and Correlation Coefficient		
	Compared Images	PSNR	Correlation Coefficient
Profile Picture	Flower.jpg and W_Flower.jpg	41	0.9971
Watermark Image	Fingerprint.jpg and RW_Fingerprint.jpg	21.7406	0.6679

From the given figures and the table, one can easily recognize that the quality of Profile Picture is not degraded after performing Digital Watermarking. But the quality of Recovered Watermark is slightly affected because the Watermarking is performed into frequency domain. The implementation of Digital Watermarking and results presented in the table are obtained by working on MATLAB. It is a most famous tool for image processing. It helps researchers by providing inbuilt functions for fast processing.

7. CONCLUSION

Everybody around the world wants their unique presence over the any network. The Unique presence provides him to freely share their personal information to their known without compromising any security issue. The goal of this research is to provide Unique Identification to individuals over the Digital Social Network. The experiment results present the possibility of Color Image Digital Watermarking

with Fingerprint as Watermark.

This research concludes that if Social Networking websites provide a Unique Identification over Digital Social Network then it can take the advantage of:

- It can easily focus on individual's activity.
- It can completely control the duplicity of an account.
- It can achieve full faith of user.
- Its Unique Identification may further be used for online transaction.
- It can stop publishing in of other's data. By providing reporting system.
- User can easily blame on others.
- Fakers cannot create any account, because it requires unique fingerprint image for identification.

8. ACKNOWLEDGE

The research work made possible by incorporating many people around, especially, would like to express my gratitude to Ms. Sarala Naidu for their language support and for help during the research.

9. REFERENCES

- [1] Steven Warburton, Stylianos Hatzipanagos, "Digital Identity and Social Media", IGI Global, ISBN: 9781466619159, Released: July 2012.
- [2] Camp, L.Jean "Digital Identity", IEEE Technology and Society Magazine, Vol. 23, Issue:3, 2004.
- [3] Matthew J. Hornsey, "Social Identity Theory and Self-Categorization Theory: A Historical Review", Social and

Personality Psychology Compass, Blackwell Publishing Ltd., pp. 204-222, 2008.

- [4] Paul A M Van Lange, Arie W Kruglanski, E Tory Higgins, "Handbook of Theories of Social Psychology", Vol 2, British Library, ISBN 978-0-85702-961-4, 2012.
- [5] Clare Sullivan, "Digital Identity An Emergent Legal Concept", University of Adelaide Press, 2011.
- [6] Fitzgerald, Brian F., Xiaoxiang Shi, Samsung, O'Brien, Damien S., & Gao, Fuping (Eds.) "Copyright law, digital content and the Internet in the Asia-Pacific". Sydney University Press, Sydney, N.S.W, ISBN: 9781920898724, 2008.
- [7] Dr. Neeraj Bhargava, Manish Mathuria "Color Image Digital Watermarking" Springer Proceeding of International Conference ICERECT Series: Lecture Notes in Electrical Engineering, Vol. 248, in press, 2012.
- [8] Dr. Neeraj Bhargava, Dr. M. M. Sharma, Abhimanyu Singh Garhwal and Manish Mathuria, "Digital Image Authentication System based on Digital Watermarking." IEEE Conference Publications of ICRCC, pp.185-189, 2012.
- [9] Mohammad Nuruzzaman, "Digital Image Fundamentals in MATIAB,"AuthorHouse 08/23/05, ISBN 1-4208-6965-5 (sc), 2005.
- [10] Ingemar J. Cox, Matthew L. Miller, Jeffrey A Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann Publishers (Imprint of Elsevier), 2008.
- [11] Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", International Conference on Intelligent Computation Technology and Automation, IEEE, 2010.
- [12] William E. Burr, Donna F. Dodson, W. Timothy Polk, "Information Security", Electronic Authentication Guideline, NIST Special Publication 800-63 Version 1.0.2, April, 2006.