Prevention of Copyright Issues of Media in Social Network

Gayathri.K.S
Mtech Student
SCT College of Engineering
Trivandrum

Tony Thomas
Assistant Professor
IIITM-K
Trivandrum

Jayasudha.J.S
Assistant Professor
SCT College of Engineering
Trivandrum

ABSTRACT
A social network is a social communication network which allows users to interrelate with anyone in the connected network all over the world. Users are allowed to share anything across the network like photos, videos, audios, text messages etc., which are accessible to other users connected to the network. Now-a-days social networks have become a daily activity in everyone's life. People share everything happening in their life through social networks with their dear ones. Owing to its heavy usage, the number of contents being shared through social networks is also increasing. As a consequence, the security and rights of shared content are getting compromised. This paper aims to protect media shared through social networks against copyright infringement and a solution to overcome the copyright violation issue using watermarking method along with a comparison to the existing watermarking techniques.

General Terms
Watermarking, Social Network, Content Identification.

Keywords
Spread Spectrum, DCT, DWT, Fingerprinting, Copyright infringement, Content sharing.

1. INTRODUCTION
Social networks provide the foundation for online communication. People use online social networks as a platform for communicating with their friends, family or others sharing something common. The interrelation of users are based on some trust relationship which includes friendship, family based relationship or anything else which aim towards some shared interests. One can view such shared items in a social network imagining his own involvement in that event. Social networks have become the primary communication channel conquering other communication modes. The usage graph of social networks has seen a sudden rise in the recent past. Social networks have narrowed the usage of telephones, emails or other modes of communication. People use social networks to share their ideas in the form of images, videos, audios or even text messages. One can even see who is online at the moment and then chat with them. Social networks are defined as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system [6].

With the ongoing popularity and usage of social networks, the contents being shared through them has also increased. Users should be registered to use social networks [5]. The registered profile information forms the backbone of social networks as they are used for identifying a user. Users can restrict access to their contents by allowing only known persons to access the content. Though many security features have been implemented in the existing social networks, contents are still getting compromised somehow.

The motivating factor for online sharing revolves around the fact that people who are close to us can know about us no matter where ever they are. For example, sharing a marriage album with friends makes it viewable for those who could not attend the function and they get a feeling that they were present at the ceremony. Social network bears some risk along with their positive usage. There is no security to the uploaded content. Anyone can use the content in his name or even tamper its content. For example, the unauthorized distribution of movies. Illegal usage of copyrighted work without permission from the author is called copyright violation. Copyright infringement occurs when the copyright owner's rights are violated.

Apart from communication, a social network has a multitude of integrated applications. For example, some organizations use a user's Facebook credentials for authentication rather than requiring their own credentials.

Fig 1: Social Networking Sites

In this paper we provide a secure method using watermarking for media sharing across online social networks. The remaining of the paper is organized as follows. Section 2 focuses on the existing media sharing sites – YouTube, Facebook and Flickr and the issues of social networks.

Section 3 highlights the two content identification technologies namely Fingerprinting and Watermarking. Section 4 updates the proposed work. Section 5 focuses on the experimental setup and quality analysis of the proposed work. Section 7 concludes the work.

2. MEDIA SHARING SITES AND ITS ISSUES

Media sharing is an approach to aggregate, upload, compress, host and distribute images, text, applications, videos, audio, games and new media through online social networks. It is an active communication tool that requires the participation of both the sender and the receiver.

There are several media sharing sites such as flikr.com, youtube.com, dailymotion.com, blip.tv, slideshare.net and so on as shown in Figure 1. The working of a media sharing site is as follows:

First the user has to create an account with one of these websites and using that account he has to log in to the particular site. User can then upload the media files. After uploading, he will be provided with a link to share the particular media file with his friends. Anyone who follows the link can view or hear the file from their web browser. The detailed view of two major media sharing sites is explained below.

2.1 YouTube

YouTube is a popular video sharing website where the users can upload, share and view videos. Video specific features provided by YouTube are playback, uploading, downloading and user comments. Associated with each YouTube video is a piece of HTML code which facilitates the video to be embedded on a page outside to that of YouTube website. This functionality enables YouTube videos to be embedded in social networking sites. YouTube employs a Google Cloud for data storage. Users can upload any video format to YouTube which is converted internally to a flash video (flv) format. Hence only systems enabled with Flash player can be utilized to view YouTube videos.

There are some limitations in using YouTube. YouTube permits an upload of any video limited to 15 minutes or less than 2GB. This limitation of uploaded content is due to the fact that YouTube uses a Google cloud. Storage of contents in a cloud is expensive. To attract uploading of more contents, they have placed a restriction on contents to be uploaded in the case of a free user. For longer uploads, one has to be a partner of YouTube. Some of the YouTube partners are Sony Pictures, Universal Music Group, Mondo Media, Machinima etc.

How does YouTube deal with a copyrighted content posted on YouTube? To deal with copyrighted violations, YouTube employs a set of sophisticated tools called 'Content ID' that helps them to locate contents loaded to YouTube and the corresponding action to be taken such as blocking it, making money from it or to take no action against such a copyright infringement. Right holders provide YouTube with their content's reference file that they own along with a metadata specifying the actual content and policies to be employed when YouTube detects a match. When a video is uploaded to YouTube, it is compared against the precomputed reference files stored in their database. If a match is found, the specified policy such as monetize, track or block the content is applied.

'Content ID' system of YouTube's is a powerful tool against copyright infringements yet there are some problems with the system. There are videos that remixed copyrighted materials. This is because the success of Content ID system solely depends on the reference files. Reference files are created based on some specific patterns or features. If the selected features of reference files can be compromised then the copyrighted video can also be uploaded as a new one. Moreover maintaining such large database is a difficult task. YouTube is completely a video sharing site. YouTube does not support uploading either audio files or images. One can only upload, download, view or comment on a video clip. It is not possible to build a relationship model with YouTube i.e. YouTube does not support social networking.

2.2 Facebook

Facebook was first developed as a school-based social network and later grown to become the most popular interactive social network in the world. Facebook provides an online platform where friends, family or business associates can get connected. Users should register their profiles to use the site. Registered users can add friends and exchange messages with each other. Users can communicate with friends and others using private or public messages and with a chat feature. Creating a profile in a particular network implies that they are allowing anyone connected to that network full access to their profile. The profile contains information about the user, his/her status whether online or offline, list of friends, photos, groups etc. E-mail notifications make users aware of the friends who chose to add them to their list of friends or when someone in their network sends a message. Facebook uses a Hadoop cloud for data storage.

Apache Hadoop is a software framework which supports distributed applications [12]. Hadoop system allows applications to work with large number of nodes. Hadoop implements a feature called map/reduce, where the application is divided into small fragments of work, each of which may be executed or re-executed on any node in the cluster. Since it provides a distributed file system, data can be stored on the various nodes. Both map/reduce and the distributed file system facilities enable the hadoop framework to automatically handle node failures.

Facebook allows its authorized users to upload only images and videos; there is no support for audio files. Though Facebook is a flexible user interface to get in touch with others (friends, family or someone with shared interest) within the network, there are some issues faced by Facebook users. Facebook impose an upload limit of 20 minutes or less than 200 MB of content.

Photos uploaded to Facebook can be viewed by anyone connected to the network. These photos can also be used by anyone without owner's knowledge. Hence there is a threat of misuse with the uploaded content. As per Facebook's terms and conditions, uploading anything to the site implies that full permission are given to the Facebook to do anything with content uploaded like using them for commercial purposes, selling the content to other people, editing the contents etc, until one deletes the content from the Facebook server.

2.3 Flickr

Flickr is an online platform for storing, searching and sharing photos. Flickr helps to organize vast amount of photos available and offers a way for the user's friends and family to tell tales on these photos. Users can access contents from Flickr without registering to the site but needed to create an account for uploading content to the site.

Flickr allows users to organize their photos into sets or groups of photos with a common heading. These sets can be displayed as a slideshow or can be shared by embedding them in other websites. Flickr supports both private and public modes for image storage. Private images can be viewed only by the uploader or to the ones he grants permission. Flickr has introduced a new system called Guest Pass, for allowing

private images to be shared by non-flickr members. Owner can send the pass via email to people with whom he wants to share his private image. Flickr uses MySQL databases hosted on Linux-based servers. Here also there is no security for the uploaded images.

2.4 Issues of Social Networks

Social networking sites are of great help to the public in getting connected with others and also to know about the world still there are some limitations like low bandwidth, content upload limitations, unsupported tracking model and copyright violations.

2.4.1 Upload Limit

Almost all social media sites impose an upload limit on user contents. Example for such sites includes Facebook with an upload limit of 20 minutes or 200 MB, Flickr with 90 seconds or 150 MB, YouTube with 15 minutes or 2GB.

2.4.2 Unsupported Tracking Model

Current video sharing sites does not have a tracking model supported. That is after uploading content; one has no control over it such as who is viewing it, modifying it etc.

2.4.3 Copyright Infringements

Anyone can download contents from media sharing sites, make some modification and claim ownership of the same. Further some contents may also be tampered. These sites are still lacking some strong piracy protection mechanisms. User specified access control need to be implemented.

3. MEDIA PROTECTION TECHNIQUES

The major issue pertinent with media sharing in a social network is to find the owner of the shared content. There are two techniques for identifying the owner of the content posted online. The two techniques are watermarking and fingerprinting [3].

Watermarking is used to determine the authenticity of a user [2]. The noise portion of the original content is modified with the watermark in such a way that the user's perception of the content is not spoiled. Watermarking is applicable for all media types such as images, audio and video. Another approach for identifying the integrity of shared content is fingerprinting. Fingerprinting uses pattern matching for its working. The two methods are elaborated in the following sections.

3.1 Fingerprinting

Fingerprinting method identifies a content based on the content's own features. Fingerprinting process works by taking an existing content, hashes it and converts it to a unique fingerprint. A small number of relevant features are extracted from the original media and they are converted to what is called a fingerprint or a pattern [10]. Such computed fingerprints are stored in a fingerprint database. Whenever a new content is found, fingerprints are computed in similar fashion. The newly computed fingerprints are compared with the existing database fingerprints. If a match is found then the media is a copyrighted one or else it is an original work. The working of fingerprinting approach is shown in Figure 2.

Fingerprinting can be applied to audio, video and text. A fingerprint is a special type of a mathematical construct called a hash. Hash is used to check the integrity of content. Large data is sent along with a hash value which is recomputed at the receiving end. If this recomputed hash value does not match with the hash value sent with the data, it is obvious that the content is altered during transmission. Good fingerprinting technologies are helpful in detecting changes to contents like cropping, rotation, color-space shifting, audio equalization, format conversion etc.

The drawback of fingerprinting method is that its success depends on the features chosen to create fingerprints. If the features are not good enough, a copyrighted work can be compromised. For example, if the feature chosen for creating a video fingerprint is the number of frames. If the system chooses to take the first, third and fifth frames as features and are converted to fingerprints. An intruder can easily modify these frames of the original video and get the copyright work compromised. Another issue is that fingerprinting approach uses a large database to store fingerprints. Maintaining such large database is very difficult.

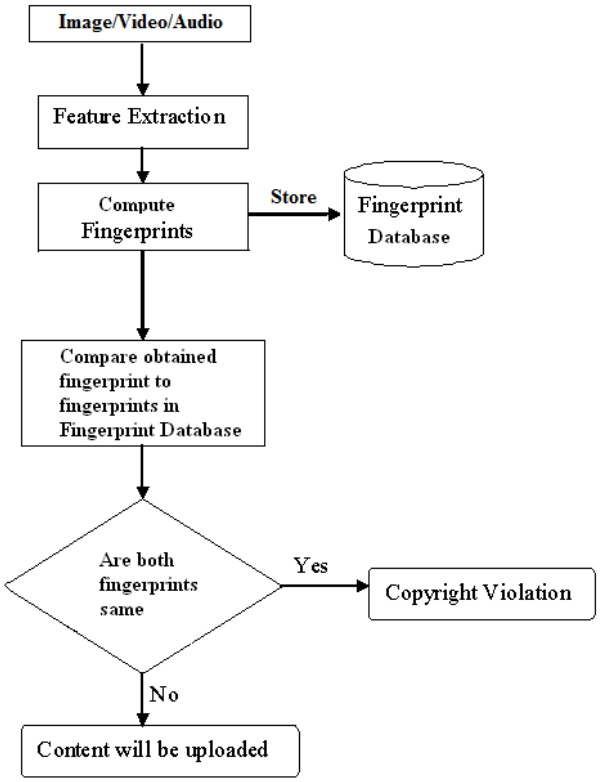


Fig 2: Fingerprinting

3.2 Watermarking

Watermarking refers to the process of hiding information in a carrier signal. The information being hidden need not contain any relation to the carrier signal. The information to be hidden can be a number or text, media contents like images, video or audio. The information is hidden by manipulating the content of the data (carrier signal). A watermark can be thought of a secondary signal being overlaid on the primary signal which aims at protecting the primary signal [8]. In the case of a digital photo, a watermark can be a logo or a text superimposed on the photo. The need for placing such a watermark on the photo is to prevent others from trying to copy and use the photo without prior permission. Currently several web-sites are using watermarks to show that a particular image is copyrighted so that it cannot be copied and used anywhere without the permission of the owner of the site on which it was displayed.

Watermarking is a powerful tool for verifying the authenticity or integrity of the carrier signal. Watermarks are perceptible in some conditions may be with the use of some detection algorithms or otherwise they are imperceptible. A watermark is called imperceptible if the original carrier signal and the watermarked signal are perceptually identical

(Invisible Watermarks) [7]. In the case of images, this means that the modifications of the pixel values have to be invisible. A watermark is called perceptible if its presence in the watermarked signal is noticeable (Visible Watermarks). The watermark does not alter the size of the carrier signal. Watermarking is a passive protection tool since both original and watermarked signal are the same.

The information to be embedded in a signal is called a watermark. The portion of the signal at which the watermark is embedded is called the host signal. Watermarking process is divided into three distinct steps namely embedding, attack and detection [9][11]. The embedding process accepts the carrier signal and the watermark and produces a watermarked signal which is similar to the carrier signal. The embedding process is shown in Figure 3.

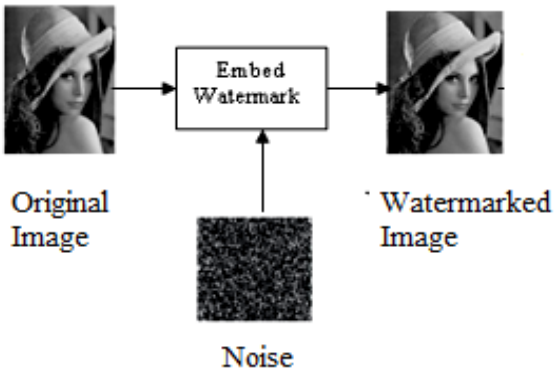


Fig 3: Watermark Embedding

The watermarked signal is then transmitted to another person. If this person tries to modify the transmitted signal, it is called an attack [17]. Modifications include cropping an image, adding noise, translation of image, compression etc. Detection/Extraction is the process where the watermarked signal is checked for the presence of watermark. This is useful in detecting attacks. If the signal was not altered during transmission, the watermark will still be present in the signal and can be extracted. The detection process is explained in Figure 4.

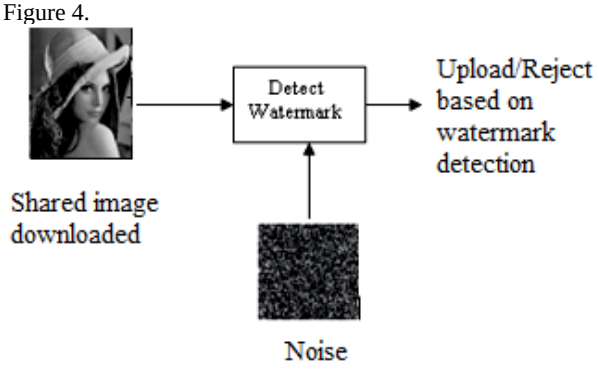


Fig 4: Watermark Detection

Watermarking process can be classified into two based on their security – Robust and Fragile [16]. In robust watermarking, the extraction of watermark should be possible even if the modifications are too strong. Robust watermarks are used for copy protection. In case of robust watermarking, the watermark should be present in the signal even after distortion. In fragile watermarking, the extraction of watermark should fail if any change is made to the signal. Fragile watermarks can be used for tamper detection.

Watermarking finds its application in several areas like copyright protection, source tracking, tampering etc. A watermark is inserted into the signal while distributing. If a copy of the work is found at some later point of time, the watermark can be retrieved from the copy and the source of the distribution of the copy can be known. This technique has been widely used to detect the source of movies or songs copied illegally. The main application of watermarking is that of copyright protection of digital media. Previously duplicating a work was quite complex and required a high level of expertise to make the forged work similar to the original. However, in the present digital world, it is possible for anyone to duplicate digital data without any lose to the data quality. Just like how artists previously signed their paintings to claim copyrights, artists of today can watermark their name within the image either visibly or invisibly. This identifies the owner of the work. The same approach is applicable to protect both video and audio being shared online. Recently there was a crisis regarding the unauthorized distribution of digital audio and video over the Internet in the MP3 format. In such a situation, watermarking acts as a useful tool for controlled audio and video distribution.

3.2.1 Watermarking Methods

Watermarking is broadly classified into two namely spatial and frequency domain based on the way watermark is embedded [12]. In spatial domain watermarking, the pixel values of the carrier signal are modified with the watermark. Example of this type of watermarking includes Least Significant Bit (LSB). In frequency domain watermarking employs computing the coefficients obtained as the result of frequency transform of an image. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are examples of frequency domain watermarking.

The idea behind LSB method is that the watermark is embedded in the LSB bit position [19]. The embedding process consists of selecting a subset (c1,…,cn) of pixel values from the cover image and applying substitution in the LSB position of the selected subset of the cover image [18][19][20]. The algorithm of LSB embedding is as follows.

Input: Cover Image C, Watermark w
for i=1 to Length (w)
Find the i^{th} index C where to embed the i^{th} bit of w
Embed w_i to LSB (C_i)
end for
Output: Watermarked Image W

In the extraction process, the LSB of the selected pixel values of watermarked image are extracted and used to reconstruct the original image. The main drawback of LSB method is that the hidden information can be destroyed by either compressing the watermarked image or transforming the image.

The discrete cosine transform is based on converting a signal into its elementary frequency components. Here an image is represented as a sum of sinusoids of varying magnitudes and frequencies.

Block-based DCT transform divides cover image into non-overlapping blocks and applies DCT-based watermarking is performed on the basis of two facts. The first fact is that at the low frequency sub-band lies much of the signal energy and so the most important visual parts of the image lies at that range. The second fact is that the high frequency sub-band of the image are mostly removed through compression and other attacks. Hence it is advisable to embed watermark by modifying the coefficients of middle frequency sub-band as both visibility and presence of watermark is not affected here. The watermark embedded image is subjected to inverse DCT to obtain a slightly modified version of original content.

DWT method decomposes the cover image into sub-image of different spatial domain and independent frequency district

[15]. After the original image has been DWT transformed, it is decomposed into 4 frequency bands namely one low-frequency band(LL) and three high-frequency bands(LH,HL,HH). A two-dimensional image after applying DWT 3 times is shown in Figure 6.

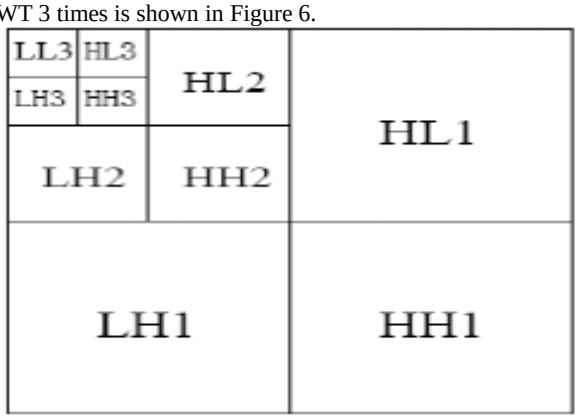


Fig 5: Sub-bands of 3-level DWT

The information in the low frequency band is similar to the original image. Most of the signal information of original image lies in this frequency band. The frequency bands of LH, HL and HH represent the level detail, the upright detail and the diagonal detail of the original image respectively. The DWT transformed result of Lena image is shown in Figure 7.

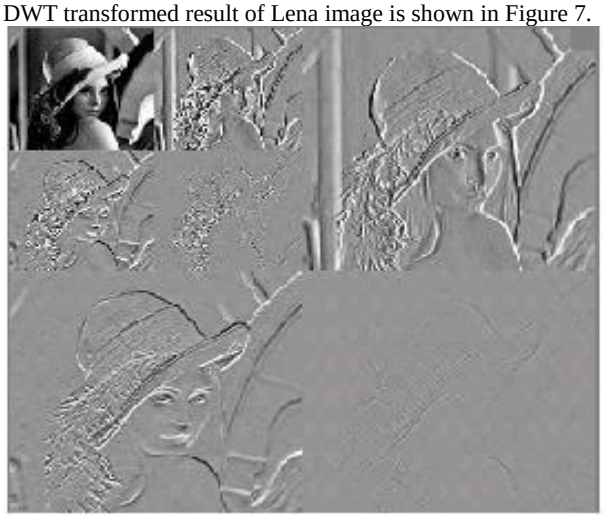


Fig 6: 3-level DWT Output of Lena

4. PROPOSED WORK

The proposed method combines three standard watermarking methods namely DWT, DCT and LSB.

4.1 Embedding Process

The cover image is subjected to single level DWT watermarking which results in four shares of frequency regions of the cover image namely LL, LH, HL and HH. LL and HH frequencies regions are not suitable for embedding watermark. In general most of the image energy is concentrated at the lower frequency band LL and hence embedding watermarks in these regions may degrade the image significantly. The HH frequency band contains the edges and textures of the image and hence trying to embed in HH bands may vary the textures and edges of the image So the advisable region to embed the watermark is either LH or HL frequency regions for improved robustness and imperceptibility. In the approach, we use the LH frequency band for embedding the watermark.

The image in the LH region is further subjected to DCT watermarking using the below equation.

$$F_{uv} = \frac{1}{4} C_u C_v \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} S_{yx} \cos\left(v\pi \frac{2y+1}{2N}\right) \cos\left(u\pi \frac{2x+1}{2N}\right)$$

where

$$C_{u=} \begin{cases} \frac{1}{\sqrt{2}} & \text{if u=0} \\ 1 & \text{otherwise} \end{cases}$$

$$C_{v=} \begin{cases} \frac{1}{\sqrt{2}} & \text{if v=0} \\ 1 & \text{otherwise} \end{cases}$$

S – input image

S_{yx} - pixel coordinates (x, y)

This results in DCT coefficients of the image in the LH frequency band. The obtained coefficients are sorted in descending order to obtain the highest coefficients. The mid-coefficient is chosen and from that position the watermark embedded. The watermark text is converted to its corresponding ASCII value and encrypted using a key and is embedded to the coefficients using LSB method. Then the embedded image is subject to inverse DCT using the below equation.

$$S_{yx} = \frac{1}{4} C_u C_v \sum_{v=0}^{N-1} \sum_{u=0}^{N-1} C_v C_u F_{vu} \cos\left(v\pi \frac{2y+1}{2N}\right) \cos\left(u\pi \frac{2x+1}{2N}\right)$$

where C_u and C_v values are as mentioned above. Inverse DWT is applied to the image to obtain the watermarked image which is slightly different from the original one. The block diagram representing embedding process shown in Figure 7.

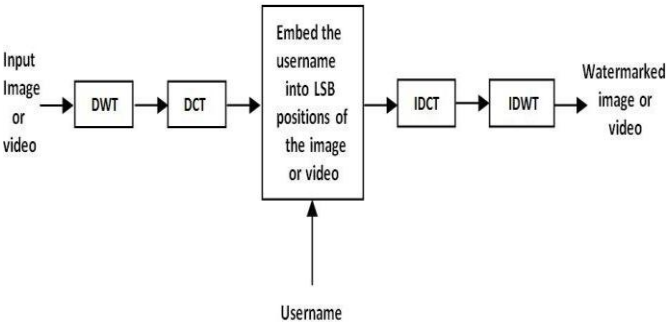


Fig 7: Block Diagram for Embedding

4.2 Detection Process

In the detection process, the watermarked image is first subjected to IDWT and the resultant image in the LH frequency band is subjected to IDCT. The coefficients obtained as the result of IDCT are sorted in descending order and the mid-coefficient is obtained. The LSB bit starting from the mid-coefficient is fetched and if it corresponds to an ASCII string then the image or video is a watermarked one and hence uploading it is against copyright violation. If there is no watermark in the image or video then it is watermarked with the corresponding username. The process is explained in Figure 8.

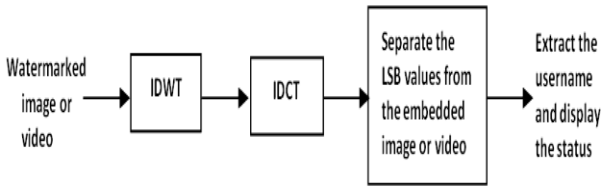


Fig 8: Block Diagram for Detection

5. EXPERIMENTS AND RESULTS

The implementation is done using ASP.Net. A social network is simulated using dotnet language. A user has to register his details for getting an account to the social network. Once an account is created, he can login to the system using his registered credentials. The social network has support for uploading and viewing images and videos. When a user uploads an image or video, the image or video is first checked for the presence of any watermark text using the proposed detection algorithm mentioned above. If no watermark text is found, then the image or video is uploaded with the user's login name embedded into it. If a watermark is detected in the video or image, the user will not be able to upload the image. In the case of videos, the video is first converted to frames. Watermark is embedded in all frames.

The proposed watermarking method is tested on both images and videos. A 225*225 jpeg Lena image is used as input for image watermarking. The original and watermarked Lena image is shown in Figure 8.

Fig 9: Watermarked Lena Image

A 320*240 Water Day2 video is used as input for video watermarking. The original and watermarked WaterDay2 video is shown in Figure 9.

Fig 10: Watermarked Video

5.1 Quality Analysis

Peak Signal to Noise Ratio (PSNR) refers to the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of the content. It is expressed in decibel scale (dB). PSNR is a standard tool to check the quality of a content. PSNR value should be greater than 30 dB for any content. The higher the PSNR value, the better is the quality of the content. PSNR of a content can be calculated using the formula

$$PSNR = 10 \log_{10} \left\{ \frac{R^2}{MSE} \right\}$$

where

R – maximum pixel value of image
MSE – mean squared error

$$MSE = \sum_{M,N} \frac{[I_o(m,n) - I_w(m,n)]^2}{M * N}$$

where

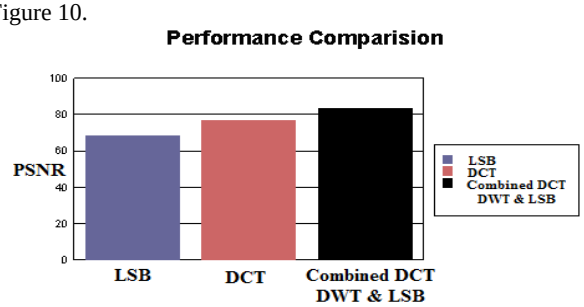
M*N – image size
$I_o(m,n)$ – pixel value in original image
$I_w(x,y)$ – pixel value in watermarked image

For videos, the PSNR value is obtained using the equation

$$PSNR = \frac{\sum_{i=0}^{N} 10 \log_{10} \frac{R^2}{MSE}}{N}$$

where N is the total number of frames in the video.

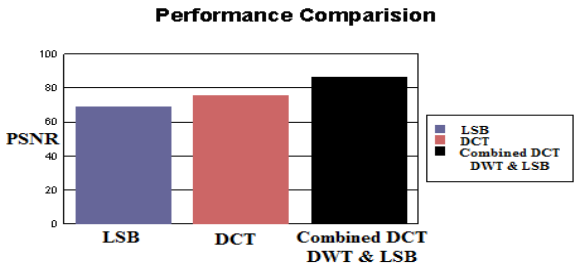
PSNR value is computed for image using the formula mentioned above. The PSNR value comparison of proposed approach with different watermarking methods like LSB and DCT using lena image is displayed in a graph as shown in Figure 10.



Method	PSNR
LSB	68.37
DCT	76.73
Combined DCT, DWT & LSB	83.28

Fig 11: PSNR Graph for Image

For videos, the PSNR value for each frame is computed all frames in the video and the total value is divided by maximum number of frames in the video. The PSNR value comparison of proposed approach with different watermarking methods like LSB and DCT using WaterDay2 video is displayed in a graph as shown in Figure 11.



Method	PSNR
LSB	68.87
DCT	75.69
Combined DCT DWT & LSB	86.79

Fig 12: PSNR Graph for Video

6. CONCLUSION

Owing to the popularity of social network, the number of people using it has also increased. This increased usage has in-turn incremented the amount of resources shared through these social networks. Hence the fear of security of these shared resources has also been raised.

This paper has provided a solution to protect resources such as images and videos being shared online of copyright violation. To prevent copyright infringement of images and videos, a content identification technology named watermarking is used. To make the watermarking more secured, a special type of watermarking called spread spectrum is used. The proposed watermarking embeds the user's name into the content uploaded. When someone else other than the owner of the content tries to upload the same content, he will not be allowed to upload it. The high PSNR value proves that the image quality is high compared with other approaches like LSB, DCT and DWT. The proposed method is highly secure as location of watermark is not obvious. Also the proposed method can withstand transformations such as rotation, scaling and cropping and even noise additions and compression attacks.

7. REFERENCES

[1] Sachan, A., Emmanuel, S., Das, A., Kankanhalli, M.S. 2009. Privacy Preserving Multiparty Multilevel DRM Architecture. IEEE Consumer Communications and Networking Conference. 1-5.

[2] Vashistha, A., Nallusamy, R. and Pau, S. 2010. NoMark: A Novel Method for Copyright Protection of Digital Videos without Embedding Data. IEEE International Symposium on Multimedia. 167-174.

[3] Rosenblatt, B. 2008. Content Identification Technology. Sun Microsystems Inc

[4] Gao, H., Hu, J., Huang, T., Wang, J. and Chen, Y. 2011. Security Issues in Online Social Networks. IEEE Internet Computing. 56-62.

[5] Zhang, C., Sun, J., Zhu, X., Fang, Y. 2010. Privacy and Security for Online Social Networks: Challenges and Opportunities. IEEE Network. 13-18.

[6] Boyd, D.M., Ellison, N.B, "Social Network Sites: Definition, History and Scholarship", Journal of Computer Mediated Communication, 2007.

[7] Mistry, D, "Comparison of Digital Water Marking methods", International Journal on Computer Science and Engineering, 2010, Vol. 02, 2905-2909.

[8] Hartung, F. and Ericsson, F.R, "Digital Rights Management and Watermarking of Multimedia Content M-Commerce Applications", Research IEEE Communications Magazine, 2003.

[9] Hartung, F., and Girod, B, "Watermarking of uncompressed and compressed video", Elsevier, 1998, Vol 66, 283-301.

[10] Lefèbvre, F., Chupeau, B., Massoudi, A. and Diehl, E. 2009. Image and Video Fingerprinting: Forensic Applications. SPIE Conference on Media Forensics and Security.

[11] Hartung, F. and Kutter, M. 1999. Multimedia Watermarking Techniques. Proceedings of IEEE. Vol. 87. 1079-1107.

[12] Borthakur, D, "Apache Hadoop FileSystem and its usage in Facebook, 2004.

[13] Cox, I.J., Kilian, J., Leighton, F.T. and Shamoon, T. 1997. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing. Vol. 6. 1673-1687

[14] Zhuhua, L., Jing, Y., Chuan, F., Guoqing, Z. 2010. A Tracking Model for Enhancing Social Video Integration and Sharing. 10th IEEE International Conference on Computer and Information Technology. 1571-1576.

[15] Jiansheng, M., Sukang, L. and Xiaomei, T. 2009. A Digital Watermarking Algorithm Based On DCT and DWT. Proceedings of the 2009 International Symposium on Web Information Systems and Applications. 104-107.

[16] Ramzan, N., Patrikakis, C., Zhang, Q., Izquierdo, E. 2010. Analysing Multimedia Content in Social Networking Environments. SAPMIA'10 ACM. 73-76.

[17] Kelkar, Y., and Shaikh, H, "Analysis of Robustness of Digital Watermarking Under Various Attacks", Multimedia Communications A Special Issue from IJCA, 2011, 47-51.

[18] Zaidoon, Kh.Al.A., Zaidan, A.A., Zaidan, B.B. and Alanazi, H.O, "Overview: Main Fundamentals for Steganography", Journal of Computing, 2010, 158-165.

[19] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. 2010. Digital Image Steganography: Survey and Analyses of Current Methods. Signal Processing. Vol. 90. 727-752

[20] Walia, E., Jain, P., Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, 2010, Vol. 10, 4-8.