# Fingerprint Model of Image Protection and Its Comparison with Various Protection Model

**Athira V Prem, Arun R Chandran**

***Abstract*-The dynamic development of the Internet causes so many bad effects on images present in the website, because images are spreading rapidly and widely. The phenomenon of image illegal usage increases day by day. It has great impact on people' s normal life. Therefore, it is very urgent to protect image security and image owner' s rights. At present, so many protection techniques are available to keep image' s privacy, but these are passive protection method. The fingerprint extraction model of image protection is very good method, it provides a better protection mechanism compared to other method. Fingerprint of an image is very unique one. Each image has its own fingerprint different from that of other image. So this technique can be used in so many social media to protect numerous images spreading day by day. Comparing with other image protection technique fingerprint protection method is very high accuracy and lower the calculation complexity required to protect the image. Future scope of this technique is to reduce the illegal usage of personal images and avoid so many fraudulent activities occurred in the busy internet world.**

***Index Terms*—fingerprint value, image fingerprinting, block of image, filtering operation.**

## I. INTRODUCTION

Over the past two decades, so many images are spreading in internet. Online image theft is a big problem arising today. In this busy internet world so many social media are present, so millions of images are spreading day by day. One of the easiest steps of protecting image against photo theft is to lower the resolution size of the photos when posting them online. It is an early method. In early days watermarking are used for this purpose. But one of the advanced versions of watermark is invisible watermark. This type of watermark act as a digital form of copyright protection for images, by embedding copyright information directly into images themselves while keeping this invisible to the naked eye. This watermark will always be enough to prevent image theft and make it easier to track down images once they have been stolen by unknown person.

But nowadays 85% of the images shared on the internet are being used without permission or license from their original creators. So preventive measures are adopted to limit, reduce the possibility of image theft occurring in the websites.

**Athira V Prem,** Electronics And Communication Department , APJ Abdul Kalam Technological University ,Kerala,India

**Arun R Chandran**, Electronics And Communication Department , APJ Abdul Kalam Technological University ,Kerala,India

One method is to prevent image theft is disable website visitors ability right click on images to prevent them from directly saving the images. But it is not effective method for protection. Another method used is hotlink protection; it is very easy when it is connected to the cloud facility. Watermark is most commonly used one technique for image protection, but it is not a great solution to the problem of image protection. The main disadvantage of this watermarked technique is that it vanishes if someone manipulates the image. Another drawback of watermarking of an image is that it cannot prevent image copying. The detection of image illegal usage is very necessary in this time. So many techniques are discovered for image protection but any of them cannot find the image illegal usage by another user and to prevent the image from other fraudulent activities. Illegal usage of image without the permission of owner is definitely a crime; such activities should be avoided to protect image owner' s right and to get the image protection in social media. This motivation is a lead to a new method of image protection is proposed. This method is fingerprint model of image protection. It is similar to the fingerprint of fingers in a human being as it is an unique value corresponding to an image.

The dynamic development of the Internet causes so many bad effects on images present in the website, because images are spreading rapidly and widely. The phenomenon of image illegal usage increases day by day. It has great impact on people' s normal life. Therefore, it is very urgent to protect image security and image owner' s rights. At present, so many protection techniques are available to keep image' s privacy, but these are passive protection method. Images which need to be protected are personal photographs, photographs of animal, bird etc. Once images are used for illegally, the image owners may suffer from great trouble or some financial loss. There are a so many images are present in various websites, and many new images appear each day. So protection of image is very necessary in this growing internet field.

### *A. Motivation*

The main motivation behind this protection method of image is very unique one compared to other techniques available now.

1. For representing the image in unique manner.
2. Protection of image is less accurate in previous method.
3. Calculation complexity increases in existing methods of image protection.

4. Image protection existing now is uses so many space to store the protected image.

### B. Objective

The main objectives are given as follows.
1. To uniquely identifies an image
2. To lower the calculation complexity while computing method.

3. To reduce the storage space required to store the protected image data.
4. To reduce the illegal usage of an image.
5. To protect an image using short memory.

### C. Overview

#### 1) Types of digital image

1. Binary image
Binary images are the simple type of images and take two values black and white or 0 and 1.A binary image is always a 1 bit image. Binary images created from the grayscale images using threshold operation.
2. Gray-scale images
Gray scale images are referred to as monochrome (one colour) images. They contain gray level information. It allows having 256 different gray levels.
3. Colour images
Colour image can be depicted by 3 band monochrome image data.Typical colour images are denoted as red, green and blue.
4. Multispectral images
It contains information outside the normal human perceptual range. This include various infrared, ultraviolet, X ray, acoustic, or radar data.
In these types of images grayscale images are used for different application.

#### 2) Image fingerprinting

Image fingerprinting is otherwise called image hashing. It is a unique and reduced code that represents the visual content of an image. Similar images can be identified using this technique.image.Similar images have similar image fingerprints. In other words image hashing the process of examining the contents of an image and then constructing value that uniquely identifies an image based on these contents. Image fingerprinting helps to manage personal photo collection and can used to detecting near duplicate copies of an image.
Using this fingerprinting of an image anyone can easily recognize if newly uploaded images are similar to previously uploaded images.Similar images can be recognized and prevent duplicate images from being used once they are uploaded. The image fingerprint can also be used to compare similarity of many images. Due to the increasing use of multimedia contents through electronic commerce and online service, the problem associated with the protection of intellectual property, management of large database and indexation of are becoming more prominent. Watermarking is considered as efficient means to these kinds of problems. But there are some issues with the use of it, such as modification of content and security. The main aim of fingerprinting is to provide fast and reliable method for content identification. If the image fingerprint differs just a bit, means that the whole images also differ a bit. The more the image fingerprints differ, it indicate that the more their visual content differs. Image fingerprinting is a technique that summarizes the perceptual characteristics of digital image into an invariant digest, and it is one of the most effective solutions for digital rights management.

#### 3) Uses of image fingerprinting

1. Image deduplication purposes**:** This is also referred to as image fingerprinting. Fingerprints of an image is typically used to avoid the comparison and transmission of bulky amount of data. Fingerprinting of image produces an output of comparatively less amount of bits. It helps to maintain security and integrity of an image.
2. Compare similarity of image**:** Image fingerprinting used to compare 2 images and checking the similarity of images**.** If the 2 images are same the fingerprint are identical and otherwise it is dissimilar fingerprint values are different from one to another. Fingerprinting function works very fastly.Instead of analysing the whole image, fingerprint value of an image is used to compare the images. Image fingerprinting is used to maintain a database and alert users when they try to upload an image for illegal pupose. It can also be used for recognizing similar images and can prevent duplicate image from being used once they are uploaded. Finding similarities of 2 images are not straight forward. Image fingerprinting is solution for such problems in this process takes relatively arbitrary amount of input and produces output of fixed size. This method is help to maintain the security and integrity of input. This method is used in many other areas of digital study such as download confirmation and encryption. Local images are used mainly used in object recognition and biometry. Image fingerprinting is a key and unique technology for biometry and image indexing. Fingerprinting is a powerful and efficient tool for media forensics. It provide accurate copy identification.
3.Video fingerprinting : It is a new method in enhanced version of image fingerprinting. In this method software identifies, take out and then condenses characteristic components of a video recording, and enabling that video to be uniquely identified by its resultant fingerprint value . This technology has proven to be a best method for identifying and comparing digital video data. Video fingerprinting is wi used interest in the Rights Management (DRM) area, particularly regarding the distribution of unauthorized content on the internet. Video fingerprinting system e content providers (eg: film studios) or publishers to determine if any of the publishers video contain content registered with the fingerprint service. If the content is detected by the publisher can take the appropriate action remove it from the site.Video fingerprinting is widely used for broadcast monitoring (news monitoring) and general media monitoring

## II. PROPOSED METHODOLOGY

Methodology of this technique is consisting of various steps. Using this method fingerprint of an image is computed using less storage space with low calculation complexity is required. An image data is high size compared with the fingerprint value. First fingerprint value of all images is computed and then it matches with the other image and find similarity between them.

*A. Fingerprint extraction model*

Fingerprint extraction module is the main element in the proposed model. The fingerprint extraction model proposed model has lower calculation complexity and high accuracy. It is the process of examining the contents of an image and then constructing a value that is uniquely identifies an image. Image fingerprinting used to help to manage personal photos from illegal usage. Image fingerprinting identifies each image. Fingerprint of an image Detect near-duplicate of an image. It minimizes the storage space because the storage needed for some numbers are smaller than that of image data. Fingerprint of an image can be computed as follows. It consists of 6 steps.

Step 1: load an image
Step 2: conversion of image into grayscale image.
Step 3: resize the image
Step 4: Filtering the image
Step 5: images are divided into blocks
6. Step 6: Dct computation

Step 1: load an image
Load an image is the first step to calculate the fingerprint of an image. The image size may varies. Normally use jpeg, png, and tiff format images for performing operation to find out the unique value.
Step 2: conversion of image into grayscale image.
The images are converted into gray scale image is the next step of the proposed methodology. Gray level image is the most used image format for image processing. It consists of shades of gray. The contrast ranges from black at the weakest intensity and white at the strongest intensity. Today' s displays and image capture hardware can only support 8 bit images. Grayscale images are entirely sufficient for many tasks and so there is no need to use more complicated and harder to process colour images. For many application of image processing, colour information doesn' t help us identify important edges and other features.color images are used the codes became complex in nature and very hard to code.For learning image processing it is better to understand grayscale processing first and understand how it applies to multichannel processing rather than full colour imaging. Another advantage of grayscale conversion is that conceptualization is very easy.
Step 3: resize the image
The image loaded is any size but fingerprint of all images should be same size. So resizing an image is necessary for the computation. Images an often make up the bulk of the bytes needed to load the web page. Resizing the image is easier to load will pay dividends in increased site speed.
Step 4: Filtering the image
The resized image is filtered for noise removal present in the image. Image filtering changes the range of an image, so the colours of the image are altered without changing the pixel position. Filtering the image is mainly used for suppress either the high frequencies in the image.Guassian filtering is used in this case. Filtering technique modify or enhancing an image data. Filter a data to emphasize certain feature or remove other features. Image filtering alter the range of an image.Filtering of an image can be done either in frequency or in spatial domain.Guassian filter is a linear filter. It is primarly used to blur the image or to suppress the noise content in it. The filter alone will blur edges and reduce contrast. One advantage of Guassian filter is that it is very faster. It is considered as he ideal time domain filter and minimum possible group delay.
Step 5: images are divided into blocks
The filtered image is divided into different types of blocks. For finding the fingerprint value of an image image is split into different parts of an image.
Step 6:Dct computation
Compute the fingerprint value of an image. It is unique for each image. Fingerprint value is a number consist of zeros and ones. Fingerprint value is otherwise called hash value of an image. For computing fingerprint value of an image dct is calculated.32*32 and 8*8 dct is calculated at last 64 bit fingerprint value is obtained as result.by using 8*8 dct function so get the 64 bit fingerprint value as result.

*B. Comparison of fingerprint protection of image with other protection method*

Visible watermarking and invisible watermarking are 2 types of watermarking used for image protection. These are used to prevent content theft. Watermarking provide robustness, because it is able to withstand after normal signal operation such as image cropping, transformation, compression etc.An unauthorized user cannot detect, retrieve or modify the embedded watermark.Implementaton on pc platform is possible by using watermarking, it uniquely identifies author. These are the main advantages of watermarking method.Comparing with the fingerprint technique the visible watermark can be easily removed.watermark sometime vanishes if someone manipulates the image in a program like photoshop.resizing,compression and converting images from one file to another may add noise to an image. So this is not an accurate image protection method.
Digital signature is one kind of electronic signature that encrypts documents with digital codes. That codes are very difficult to duplicate. It takes the concept of paper based signing technique and turns it into an electronic fingerprint.This' fingerprint' or coded message is unique to both the document and the signer and binds them together. It added security to image data. A combined digital watermarking and digita signature method is used in this time. This scheme can verify the authenticity and the integrity of images and also can locate the illegal modifications on the data. The rapid growth of Internet causes digital media has created an urgent need for copyright protection because of easy replication and modification on data.Watermark method mainly emphasize on protecting the right of service providers, but digital signature focuses on that of the customers. The main disadvantage of this technique comparing with the new fingerprint technique is it can only detect the known attacks. The signature file must kept to up to date, is very difficult in the busy world.
The other protection technique used is reversible data hiding with contrast enhancement. The main advantage over this technique compared with other technique such as watermarking and digital signature is that distortion is less. Blind data extraction and complete recovery of images are both enabled in this technique. This method requires so many calculation and complex systems models. In this calculation

of image protection need so many complex algorithms. But in Fingerprint protection of image is lower the calculation complexity for protecting an image.

Integrated model of image protection technique is one of the protection technique used in this time. It combines both Block-Permutation-Based Encryption (BPBE) and Reversible Data Hiding (RDH). The method consist of following steps for encryption, namely block scrambling, block-rotation/inversion, negative-positive transformation and the colour component shuffling. A Histogram Shifting (HS) technique is used for RDH in this type of model. The scheme can be absolutely suitable for the hierarchical access control system, where the data can be accessed with the different access rights. Main advantage is that embedding rate is maximum and severe distortion. Disadvantage of this method is decryption process is very complex in nature. So this technique is not widely used one.

Discussing with the other protection method available for image, the fingerprint method is very unique in nature and it requires less space compared with the other techniques. It lower the calculation complexity. Each image can be represented a short number but it is unique. The main application area of this method is to reduce the image illegal usage in social media.if any illegal usage of personal photographs are occurred an alert will be issued to the image owner and the owner can take remedies for the fraudulent activities.

## III. CONCLUSION

The fingerprint extraction model of image protection is very good method, it provides a better protection mechanism compared to other method. This method is also used to compare two images and compare its similarity among them. If the two images are same the fingerprint values are exactly equal one. So this technique is very useful in case of image illegal usage is happened. The existing image protection methods are less accurate, very complex calculation comparing with the fingerprint protection model of image.

## ACKNOWLEDGMENT

We thank to express sincere thanks to all faculty members of the Department of Electronics and Communication for their support, and express sincere thanks to friends for their valuable support. Last but not the least we thank **Almighty God** for abundant blessings upon in the completion of this work.

## REFERENCES

[1] Spark-based real-time proactive image tracking protection model Yahong Hu*Xia Sheng, Jiafa Mao, Kaihui Wang and Danhong Zhong Hu et al. EURASIP Journal on Information Security (2019) 2019:3 https://doi.org/10.1186/s13635-019-0086-2

[2] J.F. Mao, G. Xiao, W.G. Sheng, et al., A method for video authenticity based on the fingerprint of scene frame. Neurocomputing. 173, 2022– 2032 (2016)

[3] J. Liu, H. Wang, Image protection scheme based on privacy protection in content sharing environment. Comp. Appl. Software 32(7), 207– 211 (2015)

[4] X. Lu, X. Han, Research on big data security and privacy protection technology architecture. Inform. Secur. Res. 2(3), 244– 250 (2016)

[5] Y. Liu, T. Zhang, X. Jin, et al., Personal privacy protection in big data era. J. Comput. Res. Dev. 52(1), 229– 247 (2015)

[6] I.J. Cox, J. Kilian, F.T. Leighton, et al., Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. 6, 1673– 1687 (1997)

[7] G. Xuan, J. Zhu, J. Chen, et al., Distortionless data hiding based on integer wavelet transform. IEEE Electron. Lett. 38, 1646– 1684 (2002)

[8] H.T. Wu, J.L. Dugelay, Y.Q. Shi, Reversible image data hiding with contrast enhancement. IEEE Signal Process Lett. 22, 81– 85 (2015)

[9] H.Y. Cui, J.F. Cao, Massive scene image retrieval based on improved distribute K-Means feature clustering. J. Comput. Appl. Softw. 33(6), 195– 200 (2016)

[10] Scrapy 1.6 documentation. https://docs.scrapy.org/en/latest/. Accessed 04 Feb 2019

[11] L. Liu, Y. Ma, X. Zhang, et al., Image matching method based on binary SIFTfeature description. Comp. Appl. Softw. 33(12), 152– 155 (2016)

[12] G.X. Tan, Z.H. Liu, Learning to rank based approach for image searching.Comp. Sci. 42(12), 275– 278 (2015)

[13] L.J. Jin, Research on Content Based Image Retrieval Technology (Huazhong University of Science & Technology, Wuhan, 2018)

[14] L. Zhang, F. Zhu, H. Zhong, Interactive data preprocessing system based on Spark. Appl. Comput. 25(11), 84– 89 (2016).

[15] A.Aryal, S. Imaizumi, T. Horiuchi, et al., Integrated model of image protection techniques. J. Imag. 4(1), 1– 12 (2017)

[16] N.K. Pareek, V. Patidar, Medical image protection using genetic algorithm operations. Soft. Comput. 20, 763– 772 (2016)

[17] D.G. Feng, Z. Min, L. Hao, Big data security and privacy protection. Chin. J. Comput. Phys. 37(1), 246– 258 (2014)

**Athira V Prem** Received B.Tech degree in Electronics and Communication Engineering in 2017,Cochin University of Science and Technolgy at College of Engineering Attingal,Trivandrum and pursuing M.Tech in Wireless Technology,APJ Abdul Kalam Technological University at College of Engineering Kidangoor,Kottayam,Kerala.

**Arun R Chandran** is an Assistant Professor in Electronics and Communication Engineering, APJ Abdul Kalam Technological University at College of Engineering Kidangoor,Kottayam,Kerala.