IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. II (May-Jun. 2014), PP 73-77
www.iosrjournals.org

A Survey Of Sign Based Image Copy Detection Methods

Ms. Payal R. Shete, Mrs. Girija G. Chiddarwar
Department of Computer Engineering, Sinhgad College of Engineering, Pune, India.
Department of Computer Engineering, Sinhgad College of Engineering, Pune, India.

Abstract: *The world wide web is filled with billions of images and redundant copies of images can frequently be found on many websites. These duplicates can be exact copies or differ slightly in their visual content. To assure privacy it is mandatory to preserve copyright verification, image-content identification, copy detection and authentication. This paper provides a comparative study on how content-based image copy detection methods are used to detect the copy of original image. The methods based on content based copy detection which includes signs of discrete cosine transform (DCT) and discrete wavelet transform (DWT), color histograms, by using concept of dual signature are presented.*
Keywords: *Copyright, Content Based Image Copy Detection, Redundancy, Discrete Wavelet Transform.*

I. Introduction

The success of the Internet and cost-effective digital storage device has made possible to replicate, transmit, and distribute digital content in an effortless way. Thus, the protection of intellectual property right (IPR) has become a crucial legal issue [2]. Detecting copies of digital media (images, audio and video) is a basic application of copy detection which includes usage tracking and copyright violation enforcement.

There are two approaches to protect copyright on digital image; watermarking and content-based copy detection. Watermarking embeds information or watermark into the image before distribution. Thus, all copies of the marked content contain the watermark, which can be extracted further to detect ownership. In the advance case, it is content-based, which means it does not require additional information but image itself. Generally, an image contains enough unique information that can be used for detecting copies, especially illegally distributed copies.

Storing personal data on third party database servers gives rise to many privacy and security concerns. This necessitates the protection of data and the ability to process multimedia data in the protected domain efficiently. This paper summarizes main approaches and point out interesting parts of the image copy detection methods.

Billions of images can be found on the internet, number which is growing day by day. Anyone browsing the different sites will quickly encounter many duplicates of images in multiple locations [3]. For example, the same photo of the Tajmahal of an Agra may be used by several news sources and books, while the same funny image of a baby dressed up like a elephant may be shared by hundreds of people on a social network. In general, being able to detect and track duplicates is useful in many different application areas, including:

Storage space reduction: Instead of keeping a multiple copy of same file only a single image needs to be stored, which is particularly unique and reduce storage space.

Detection of Intellectual Property Rights (IPR): Rights holders should have the privilege to discover where on the web their images are illegitimately used.

Understanding behavior and interests: Tracking how images are shared and how they spread across the internet can give insights into the social behavior of people and their interests.

It is necessary to analyze that how well content based image copy (duplicates) detection methods are able to detect the copy of a query image. Duplicates can be either exact duplicates, indicating the images are completely identical in content, or near-duplicates [3], indicating the images are not identical but differs slightly in content. Survey does not make an explicit distinction between these two types and simply use the term duplicates to refer to them both.

The typical content based copy detection system is mainly divided into three main parts. The first one is database side, second is query side and third is dataset. The images in the collection is firstly given as input to the database side which is further converted into a particular image representation that can optionally be stored in an indexing structure. The next step is to store this structure into the database. Finally, once a query image has been received, the system can use the indexing structure to restrict the search to only those images most likely to be duplicates of the query. These duplicates are derived on the basis of similarity measurements.

The focus of this paper is on image copy detection, and the rest of the paper is organized as follows. In Section 2, review of the multimedia security techniques and their appropriateness for image copy detection is given. Section 3 provides a detailed presentation of paradigms and methods. Different categories of image copy detection are explained in Section 4. Discussion and conclusion follow in Sections 5, respectively.

II. Multimedia Security

Multimedia security is the important term while dealing with the multimedia data. It is necessary to ensure that the data we are storing or using must be secured. The multimedia security can be further divided into three categories [2]: System works on the classical cryptography, other works on watermarking and third works on content fingerprinting. Watermarking is traditionally done for the purpose of copyright [3]. The purpose of content fingerprinting is the monitoring and indexing the content [4] while encryption as a part of cryptography is used to achieve the data integrity and user privacy [5].

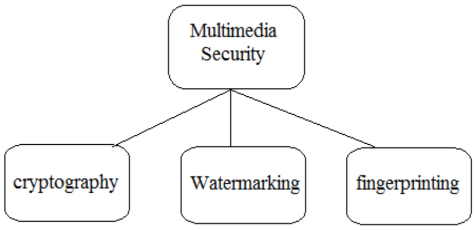


Figure 1: categories of Multimedia Security

A. Cryptography

The art of protecting information by transforming into an unreadable format (encrypted), called cipher text. Only those who possess a secret *key* can decipher (decrypt) the message into plain text [3]. Encrypted messages can sometimes be broken called code breaking. In modern days, cryptography techniques are used in credit cards, ATM cards, computer passwords and e-commerce.

B. Watermarking

Digital watermark is a kind of marker covertly embedded in a noise-tolerant signal [1] such as audio or image data. It is typically used to identify ownership of the copyright of such data, image or video. Traditional Watermarks applied only to visible media like images or video, whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models.

C. Content fingerprinting

Content fingerprinting [5] is nothing but monitoring and indexing of media content. It is a technique in which software identifies and extracts the characteristic component of media, enabling that the media to be identified by its resultant fingerprints. This is effectively used in Digital Rights Management (DRM) particularly regarding the distribution of unauthorized content on the Internet.

III. Paradigms and Methods

From analysis of the literature [3] four main paradigms are identified, namely on image representations based on (i) transforms, (ii) histograms, (iii) intensity, and (iv) structure. Looking more closely at above different paradigms, we can further categorize them based on the techniques used

Transforms: This method primarily applies one or more signal transform to images to obtain the image representations. The literature survey on copy detection shows that the discrete cosine transform and the discrete wavelet transform are predominantly used, although the Fourier-Mellin transform has been gaining traction in recent years.

Histograms: This is nothing but the paradigm which represents images by histograms, which calculate the distribution of pixels by arranging them into a number of discrete intervals. This property makes them suitable for detecting scenes that visually look similar, but when it comes to the smaller scale without additional measures they are unable to capture dissimilarities.

Intensity: This paradigm mainly focuses on the methods like grayscale image properties such as intensity, contrast, and luminance. Intensity-based methods, due to their dependence on these image properties, have to incorporate measures to ensure they are robust to changes in illumination and noise.

Structure: In the structure paradigm duplicates are detected by matching the spatial composition of images to each other, where its associated methods are generally built upon filters that locate salient details in the visual content and then use this knowledge to construct models of the spatial layout of the image. Here we can differentiate between methods exploiting the structure of the image from a global point of view, which aim to ensure that the dominant spatial structure of duplicates corresponds, or from a local point of view, which try to find matches between individual salient details.

The Table 1 presents the classification of paradigms and methods. The table shows the suitable representative methods for the paradigms [4] of transforms, histograms and structure, third column represents the references of the paper for further details of actual implementations.

Paradigm	Aspect	References
Transform	1. Discrete cosine transform (DCT) 2. Discrete wavelet transform (DWT)	[6] [7]
Histogram	1.Color probability 2. Color pyramid	[8] [9]
Intensity	1.Intensity differences 2. Intensity variances	[10] [10]
Structure	1. Global structure 2. Local structure	[11] [12]

Table 1.Classification of Paradigms and Methods

IV. Image Copy Detection

Currently, the image copy detection schemes can be classified into different categories. One is content-based image copy detection and the others are CBICD using sign of DCT, DWT coefficient and CBICD using dual signature

A. Content Based Image Copy Detection

The content based copy detection can be used in a two ways. Firstly it is used as novel content based image copy detection [1] and another approach is to use it with the watermarking [6].

The concept of content based copy detection is proposed for identifying the illegal copies of the original image. The goal behind this is to detect the true copy by its image itself instead of hiding additional information into it [1]. The working of the content based copy detection is as follows: Consider an image registered by the owner; the system can determine whether replicas of the image are available over the Internet or through any unauthorized third party. If it is found that an image is registered (i.e., it belongs to a content owner), but the user does not possess the right to use it, the image will be deemed as an illegal copy. The suspect image is then sent to the content owner for further identification and decision about taking legal action against the user. The literature survey to this topic shows that some researchers consider the content-based copy detection is a kind of content-based image retrieval (CBIR) [11].

The content based copy detection can also be used as a complementary approach to watermarking. The following procedure shows the use of watermarking with content based image copy detection. Here actual owner of the media add the watermark or embed the signature into data to prove the ownership. The next step is to extract watermark [16] from the original image and as well as from the test image and then finally compare both the watermarks to know the result [6].

The key advantage of using content based image copy detection over watermarking is that the watermark or signature extraction is not required to be conducted prior to image distribution. A challenge is that query copies may not be same as the original image. A third party may generate slight modifications to dodge copy detection or enhance image quality.

B. Content Based Copy Detection Using Sign of DCT and DWT Coefficient

The content based copy detection is intended to detect the image copies. The CBCD must resist to the specific image alteration such as, noise addition, compression, contrast and gamma changing, resizing and slight shifting. The CBCD proposes an efficient method based on the sign of the discrete cosine transform (DCT) [13] coefficient of the DC image [13].

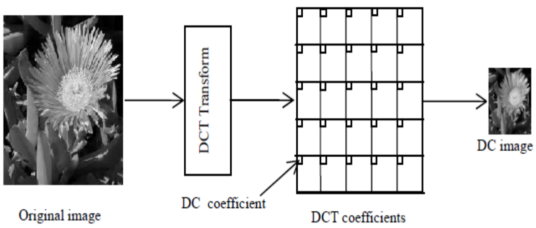


Figure 2: Generation of a DC Image

The method uses the positive and negative signs of DCT coefficients of one image, known as DC image. The DC image is generated using only DC components of blocked DCT coefficients of the original image. The size of features for representing an image can be minimized as low as 48 bits/image. The proposed method is superior in efficiency and accuracy to MPEG-7 color layout descriptor (CLD) [5] consisting of 63 bits/image.

Another way of applying the content based image copy detection is by using the sign of wavelet coefficient. The diagram below shows the basic image retrieval system in copy detection:

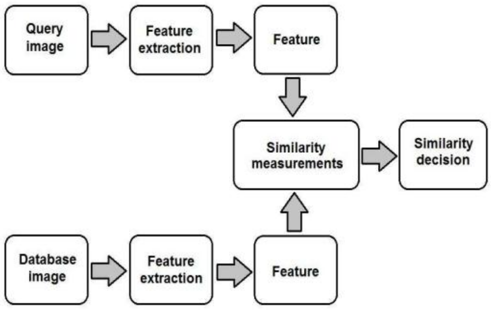
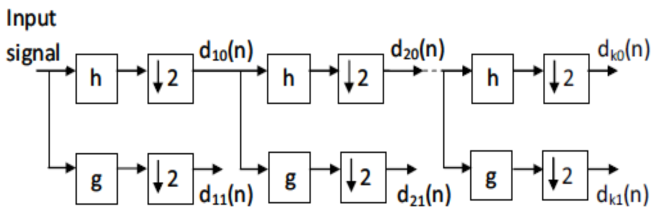
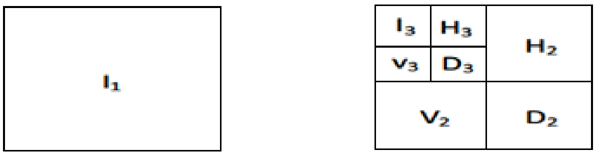


Figure 3: Block Diagram of Image Retrieval System for Copy Detection

Discrete wavelet transform (DWT) [6] is a core processing in JPEG2000 image compression standard. The wavelet provides many different capabilities like multi resolution, good energy compaction and adaptability to human visual system [14]. Wavelet transform represent signal as a superposition of family of basis function called as wavelet.



- $d_{10}(n)$ lower band signal at level i.
- $d_{11}(n)$ higher band signal at level i.



a. Result Of Two Level Decomposition Applied To An Image
Figure 4. Wavelet Transform of Image [14]

The figure 4 represents the wavelet transform of the image where input signal is passed to the low and high pass of the filter and output of that is again divided into two. Output of the low pass filter which then passes into the same process, the procedure is repeated until we get the several level of decomposition. DWT uses the separable approach where rows and columns are passed to the filter separately. The results are shown into the two level of decomposition which creates the parts of the image as I_1, I_3, H_3, V_3, D_3, H_2, V_2, D_2.

C. Content Based Copy Detection Using Concept of Dual Signature

This concept makes a focus on image feature extraction from DCT coefficient of an image at the same time check the capabilities of the image detecting the copies while resisting to some common image alteration. The image is represented by the two dimensional DCT coefficient which is nothing but the data with real values and composed of two parts one is sign part and another is magnitude part [15]. The dual signature stands for the two type of signature encoded in the image. Among them first one is the extraction of sign signature and second one is extraction of ordinal signature. Based on above signature types the dual signature concept works in content based copy detection domain. The similarity of the two images is calculated with the help of formulas called as similarity measurements. Let us define Q and D as a query image and a database image, S_Q and S_D as their Sign signatures, O_Q and O_D as their Ordinal signatures respectively. Given that Sign signatures have ternary values, the similarity between two Sign signatures is calculated as [15]:

$$simil_{Q,D}(\%) = \left(\frac{\sum_{l=1}^{L} S_Q(l)S_D(l)}{\sum_{l=1}^{L}\left|S_Q(l)S_D(l)\right|} + 1\right) * 50$$

Where *L* is the size of the signature array. Note that $simil_{Q,D}$ metric may vary from 0% to 100%. The maximum value (100%) is achieved when all corresponding positions with non-zero values have the same sign. Conversely, the minimum value (0%) is reached when all corresponding position with non-zero values have opposite signs.

V. Conclusion

In the proposed paper, we have discussed and compared various sign based image copy detection techniques. Survey analyzed the multimedia security as well as paradigms and methods and their respective types to gain further insight strengths and weaknesses of the paradigms. It is observed that to obtain high accuracy content based copy detection is best used over watermarking. This is because it does not require extracting watermark prior to storage or distribution.

This paper represents various copy detection techniques like DCT, DWT and Dual Signature with their different aspects and goal in detail. All the techniques have been individually proposed and have various advantages and disadvantages accordingly. By concatenating any two methods from the above will help us in advancement of future scope.

References

[1] Y.H. Wan, Q.L. Yuan, S.M. Ji, L.M. He,Y.L. Wang “A survey of the image copy detection” Zhejiang Province NSF Grant # Y106332 IEEE Zhejiang University of Technology Hangzhou, China 2008

[2] M. Diephuis, S. Voloshynovskiy_, O. Koval and F. Beekhof IEEE “DCT Sign Based Robust Privacy Preserving Image Copy Detection for Cloud-based Systems” Stochastic Information Processing Group, Universit´e de Gen`eve 1227 Carouge, Switzerland {Maurits.Diephuis, svolos, Oleksiy.Koval, 978-1-4673-2369-7/12 2012.

[3] Bart Thomee Mark J. Huiskes Erwin Bakker Michael S. Lew, “Large Scale Image Copy Detection Evaluation” LIACS Media Lab, Leiden University Niels Bohrweg 1, 2333 CA Leiden, The Netherlands. *MIR’08*, October 30–31, 2008, Vancouver, British Columbia, Canada. Copyright 2008 ACM 978-1-60558-312-9/08/10

[4] J. Haitsma and T. Kalker, “A highly robust audio fingerprinting system with an efficient search strategy,” Journal of New Music Research, vol. 32, no. 2, pp. 211–221, 2003.

[5] D. Engel, T. St¨utz, and A. Uhl, “Analysis of jpeg 2000 encryption with key-dependent wavelet packet subband structures,” 2010.

[6] C Kim, “Content-based image copy detection,” SPIC, pp. 169–184, 2003.

[7] E Y Chang, J Z Wang, C Li, and G Wiederhold, “RIME: A Replicated Image Detector for the World-Wide Web,” SPIE,vol. 3527, pp. 68–77, 1998.

[8] N Sebe and M S Lew, “Color-based retrieval,” Pattern Recognition Letters, vol. 22, pp. 223–230, 2001.

[9] O Chum, J Philbin, M Isard, and A Zisserman, “Scalable Near Identical Image and Shot Detection,” CIVR, pp. 549–556, 2007.

[10] B Thomee, M J Huiskes, E M Bakker, and M S Lew, “Large scale image copy detection evaluation,” MIR, pp. 59–66, 2008.

[11] MDouze, H J´egou, H Sandhawalia, L Amsaleg, and C Schmid, “Evaluation of GIST descriptors for web-scale image search,” CIVR, p. 19, 2009.

[12] B Thomee, E M Bakker, and M S Lew, “TOP-SURF: A visual words toolkit,” MM, pp. 1473–1476, 2010.M.

[13] F. Arnia, K. Munadi, M. Fujiyoshi, and H Kiya, “Efficient content-based copy detection using signs of dct coefficient,” vol. 1, pp. 494 –499, oct. 2009.

[14] Fitri arnia, agustinus Ifan, khairul munadi, Massaki fujiyoshi, hitoshi kia, “Content based image copy detection based on sign of wavelet coefficient”, International Workshop on Advanced Image Technology 2011 January 7-8, 2011.

[15] Nadia Baaziz and Maxime Guinin,“Content-Based Image Copy Detection Using Dual Signatures”, 978-1-4673-0753-6/11/$26.00n©2011 IEEE École Nationale Supérieure d’Ingénierie de Caen (ENSICAEN), 14050 Cedex 04 France

[16] Bart Thomee Mark J. Huiskes Erwin Bakker Michael S. Lew, “Large Scale Image Copy Detection Evaluation” LIACS Media Lab, Leiden University Niels Bohrweg 1, 2333 CA Leiden, The Netherlands.
MIR’08, October 30–31, 2008, Vancouver, British Columbia, Canada. Copyright 2008 ACM 978-1-60558-312-9/08/