A Survey of the Image Copy Detection

Y.H. Wan1,2, Q.L. Yuan1, S.M. Ji1, L.M. He2, Y.L. Wang1

1. The MOE Key Laboratory of Mechanical and Automation
Zhejiang University of Technology
Hangzhou, China
wanyuehua@zjut.edu.cn

2. Library of Zhejiang Univ Technol
Zhejiang University of Technology
Hangzhou, China
yuanql@zjut.edu.cn

Abstract—This paper presents a review of recent as well as classic image copy detection method. The reviewed methods are classified as digital watermarking and contended based copy detection. The contended based copy detection usually extracts robust features from image directly that is the main difference from the digital watermarking which features are embedded before distribute. Some new and key techniques are discussed that applied in watermarking and CBED. Main contributions, advantages, and drawbacks of the methods are mentioned in the paper. Problematic issues of image copy detection and outlook for the future research are discussed too. The major goal of the paper is to provide a comprehensive reference source for the researchers involved in image copy detection, regardless of particular application areas.

Keywords—Review, content based, copy detection, watermarking, feature extraction

I. INTRODUCTION

The rapid growth of the Internet has made the digital media acquiring and distributing easy in daily life. As digital image can be copied and modified easily, protecting the copyright of the digital media especially the digital image has become an important topic. Existing solutions rely either on the use of watermarks (see [1]) or on features extracted from the content itself. Each of these alternatives has specific advantages and drawbacks. Watermarks can include various useful meta-data and can keep the computational costs of copy detection relatively low, but are not very robust to image transformations (blur, crop, add logos or frames, resize, etc.). Also, watermark-based copy detection cannot be used if copies of the original content were disseminated before the application of any mark, which is unfortunately the case for a large part of the existing content. Recent content-based copy detection (CBCD) methods for still images and video (e.g. [2]-[5]) do not depend on the presence of marks and are more robust to image transformations.[6] More and more researchers focus on this aspect, many image copy detection techniques have been proposed in the past decades. According to the database of the Institute of Scientific Information (ISI), EI, ISTP, and INSPEC, in the last 10 years more than 300 papers were published on the topic of image copy detection or copy protecting. But there is not a comprehensive survey of image copy detection methods by now. The intention of our article is to cover relevant approaches introduced later and in this way map the current development of image copy detection techniques. We do not contemplate to go into details of particular algorithms or describe results of comparative experiments, rather we want to summarize main approaches and point out interesting parts of the image copy detection methods.

In Section 2, the image copy detection methods are classified into two categories: watermarks based and contended based approaches and various aspects and problems of each approach will be discussed. Section 3 reviews the existing algorithms for feature extraction or generation. Section 4 how to decide whether the query image is an illegal copy of the original image, this section actually discusses feature matching. Section 5 discusses the robust of the existing detection methods. The paper concludes at the level of systems: indexing, system architecture, and evaluation of performance. Each chapter is concluded by a discussion on the state of the art.

II. CATEGORIES OF THE IMAGE COPY DETECTION

Currently, the image copy detection schemes can be classified into two categories. One is watermarking and the other is content-based image copy detection.

A. Digital watermarking

Digital watermarking was the first solution developed to prevent the abuse of digital images. Many digital watermark schemes, such as spectrum watermarks [8], quantization watermarks [9], and blind detection watermarks [10], have been proposed to protect digital images. A digital watermark is basically an identification code that carries information about the copyright owner. It can be invisible and permanently embedded in digital data for copyright protection, ownership verification, and integrity verification.

Generally speaking, the effectiveness of a watermark-based copy detection system depends on a large extent on the robustness of the associated digital watermarking method [11], [12]. Middle frequency of wavelets transform as most people know, it has good performance on balance the robustness and blindness. But Joo et al. [19] proposed a scheme that embeds the watermark into visually insensitive location of low frequency domain to achieve good robustness and meet the blindness also. So the research of embedding watermarks transfer to low frequency from middle frequency. Lou et al. [23] applied visual cryptography technique to copyright protection scheme that improved the robustness and blindness synchronously.
B. Contended based copy detections

Recently, the concept of content-based copy detection has been proposed as an alternative means of identifying illegal image copies. The idea is that, instead of hiding additional information in an image to enable copy detection, the image itself can be employed for the same purpose. A content-based copy detection system works as follows: given an image registered by the owner, the system can determine whether near-replicas of the image are available on the Internet or through an 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 have the right to use it, the image will be deemed an illegal copy. The suspect image is then sent to the content owner for further identification and a decision about taking legal action against the user. Some researchers consider that the content-based copy detection is a kind of content-based image retrieval (CBIR) [13]-[16], which is widely used to retrieve desired images from a large collection of images. Nevertheless, there is a difference between CBCD and CBIR. Image copy detector searches for all copies of a query image, whereas a CBIR system searches for similar images, usually in terms of color [7]. CBCD can, thus, be treated as a restricted case of CBIR. However, it is not usually feasible to apply existing CBIR techniques to CBCD because they may cause a considerable number of false alarms. CBCD can be used to distinguish illegal copies on its own, or it can complement digital watermark techniques. One way to combine the two methods is to employ a copy detector to find near-replica images initially, and then extract the digital watermarks to confirm ownership. [17]

However, CBCD methods have a higher computational cost, so scalability is more difficult to achieve.

III. THE KEY TECHNIQUES OF COPY DETECTION

A. Methods for embedding watermarks

Many watermarking techniques have been proposed in the past decades which can be classified into spatial-domain or transform domain techniques. But now the watermark is often embedded into the transform domain rather than the spatial domain due to the watermark embedded into the transform domain has higher robustness.

An earlier technique proposed by Cox et al. [18] selects 1000 DCT coefficients except DC one for embedding the watermark to the achieve the requirements of robustness and imperceptibility. He proposes a watermark whose structure consists of k i.e. random numbers drawn from a distribution. The length of the watermark is variable and can be adjusted to suit the characteristics of the data. Fig. 1 illustrates the general procedure in this paper for frequency domain watermarking. Each coefficient in the frequency domain has a perceptual capacity, that is, a quantity of additional information can be added without any (or with minimal) impact to the perceptual blindness of the data.

In his paper, he recommends that the watermark be placed in the perceptually most significant components of the image spectrum [18]. Experiment results show that this algorithm can extract a reliable copy of the watermark from image that degraded with several common geometric and signal processing procedures. These procedures include translation, rotation, scale change, and cropping. The algorithm also displays strong resilience to lossy operations such as aggressive scale changes, JPEG compression, and dithering and data conversion.

The main defect is that the scheme of Cox et al. requires the original image to extract the watermark. Moreover, security is also another serious problem [21].

Wang et al. [36] proposed a wavelet-based watermarking scheme which embeds the scrambled watermark into the middle frequency of wavelet domain. The watermarks used in Wang et al.’s algorithm are real-numbered image transferred from binary images. The detailed steps of their watermark embedding algorithm are illustrated as follows:

Firstly, based on the size of the image and the watermark pattern, the number of decomposition levels L is determined. Secondly, 2L+2 sets of orthonormal filter banks are randomly generated and the wavelet decomposition pyramid is chosen also. Lastly, the analysis filters are used to decompose the image, and then the coefficients of selected middle frequency band are replaced by the watermark image.

It basically meets the requirements of the security and blindness. The main defect is that when their scheme suffers from some serious attacks, the extracted watermark is ambiguous.

Joo et al. [19] proposed a more robust wavelet-based technique than the scheme of Cox et al. [18]. The middle frequency range is known to provide a good balance between robustness and blindness [18, 22], so the DC area is excluded from consideration for watermark embedding, even though it can provide the most robustness. In [19], a reference DC’ generated from original DC is used for embed binary watermarks that were embedded into the locations with small differences between DC and DC’. In another word, this scheme embeds the watermark into low sub-band of wavelet domain by selecting visually insensitive location to meet the blindness. The experimental results show that this embedding scheme is more robust against non geometric attacks than other methods. Table 1 shows the detection precision of various methods.

<table>
<thead>
<tr>
<th>Methods</th>
<th>Detection precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang</td>
<td>74%</td>
</tr>
<tr>
<td>Cox</td>
<td>90%</td>
</tr>
<tr>
<td>Kim</td>
<td>84%</td>
</tr>
<tr>
<td>Joo</td>
<td>93%</td>
</tr>
</tbody>
</table>

The main defect is that it requires the original image to extract the watermark. In addition, the result of repeatedly embedding the watermark is time-consuming.

Der-Chyuan Lou et al. [23] proposed a robust copyright protection scheme, in that the watermark does not require to be
embedded into the protected image but is used to generate a secret image and a public image by using the visual cryptography technique. Then the secret image is registered to a certified authority (CA) for further protection. In the step of watermark extraction, the watermark can be acquired by performing exclusive-or (XOR) operation between the secret image and public image. This method is robust to withstand several image processing attacks such as JPEG lossy compression, cropping, noise adding, sharpening and blurring attacks. The main defect is that it needs the codebook to generate the secret image and extract the watermark. So even if only a byte of wrong occurs in process, the result will be changed greatly.

B. Feature Extraction in CBCD

- Global image features

To the best of our knowledge, the work of Chang et al. [24] was the first to study CBCD. It proposed a near-replica search engine called RIME (Replicated IMage dEtector) for detecting unauthorized copies of images on the Internet. The authors used wavelet and color space extract features of images. Subsequently, a clustering technique [25] was developed to improve the efficiency of RIME. Although the method can detect slightly modified images with a high degree of accuracy, it may have difficulty identifying seriously distorted images.

In 2003, Kim [7] applied the discrete cosine transform (DCT) technique to CBCD. In Kim’s scheme, images in arbitrary formats were converted to YUV format, and only Y component was used since the color does not play an important role in copy detection whereas it’s a crucial feature in the image retrieval system. The ordinal measure of DCT coefficients was used as features to represent images. In detail, the magnitudes of AC coefficients of an 8 × 8 sub-image are ranked in the descending (or ascending) order that is called a rank matrix. To measure the correlation between two rank matrices, the distance metric \(d(r_i, r_j)\) is defined as:

\[
d(r_i, r_j) = \|r_i - r_j\|_1 = \sum_{l=1}^{N} |r_{il} - r_{jl}|, \quad \forall (r_i, r_j) \in S_N
\]

where \(N\) is the size of the rank matrix.

The feature extraction procedure in Kim’s paper is shown in Figure 1.

Kim’s algorithm of ordinal measure of AC magnitudes of an 8 × 8 sub-image is summarized as follows:

1. A gray-level input image is divided into 64 (8 × 8) equal-sized sub-images (or blocks) and their average intensities are derived.

2. The derived average intensities are transformed into a series of coefficients by performing an 8 × 8 two-dimensional (2-D) DCT.

3. For ordinal measure of AC coefficients, a 1 × 63 rank matrix is generated, which contains the ranks of 63 AC magnitudes.

4. Let the rank matrix of the original (query) image \(Q\), be \(q = [q_1, q_2, \ldots, q_N]\) and that of a test image \(T\), \(t = [t_1, t_2, \ldots, t_N]\), where \(N=63\), at this moment. Then the ordinal measure between two images \(D(Q, T)\) becomes L1 norm between two rank matrices, i.e.

\[
D(Q, T) = d(q, t) = \sum_{i=1}^{N} |q_i - t_i|
\]

Kim’s experimental results showed that the use of an ordinal measure of the DCT coefficient is more robust for resisting image modifications and attacks. He successfully detected the copies both with and without modifications, especially successfully detected the copies with histogram equalization or contrast enhancement. In addition, his scheme can detect copies with general image processes, such as water coloring, motion blurring, mosaic tiling, Gaussian noise, resizing, rotated with 180°, and flipped processes and so on.

In 2005, Wu et al. [26] discovered that the rotation manipulation could make some border pixels shift to another block, so the average intensities could not accurately represent the relative blocks in Kim’s method. They proposed an elliptical track division strategy to extract two kinds of features to avoid that detects. Their feature extraction algorithm is summarized as follows:

1. Convert image to YUV color model and save the Y component.

2. Divide the image into \(N\) elliptical track blocks and derive the track mean value of each block.

3. Divide the track mean value by the image mean value to signature value

The experimental results confirm that the proposed methods can successfully capture the features of an image even when it is shifted, cropped or rotated to any degree. This method is good for detecting rotated copies but not so effective for detecting some general image processes such as water coloring and mosaic tile.

In 2006, Wu et al. [27] using a sliding window to extract image features of query and test images for overcome defects of their previous algorithm. The flowchart of their signature extracting procedure presented in Figure 2, and summarized as follows:

![Figure 1. A block diagram for feature extraction.](image-url)
1. Divide I into \( N \times N \) blocks and get the set of blocks \( \{B_0, B_1, \cdots, B_{N \times N - 1}\} \).

2. Calculate the mean value for each block and get the set of mean values, \( \{M_0, M_1, \cdots, M_{N \times N - 1}\} \).

3. For each block \( B_i \) do

(1). Extract the set of relative coefficients \( \{r_{ij}, r_{ij}, \cdots, r_{ij}\} \) with regard to the neighboring 8 blocks according to Formula (3).

\[
\begin{align*}
    r_{ij} & = 1, \quad \text{if} \quad M_i > M_{ij}, \\
    r_{ij} & = 0, \quad \text{otherwise},
\end{align*}
\]

(3) Where \( 0 < j < 7 \).

(2). Save these relative coefficients into the signature database for \( B_i \).

Their experimental results show that the scheme successfully detected the copies with 270° or 90° rotation which can not be detected by Kim’s scheme, and also can detect the copies with other modifications as same as that in Kim’s scheme. But the number of their extracted signatures is dependent on the block size, so the success rate will be affected by the block size in their proposed scheme.

- local region features

The use of global image features, as introduced above, may limit the performance of copy detection methods, since only images that are globally similar to the query image will be returned. To resolve this problem, some local region features have been used to detect local content copies. Amsaleg et al. [13] and Berrani et al. [5] use local descriptors to capture the characteristics of images. They compute many descriptors for each image, where one descriptor corresponds to a region of interest in the image. In [3], Yan et al. propose a part-based image copy detector. First, they use a difference of Gaussian (DoG) detector to construct Gaussian pyramids and then search for scale-space extrema (i.e., key points) by scanning the image over locations and scales. The key points are represented as local descriptors by using PCA-SIFT (principle components analysis on a scale-invariant feature transform). PCA-SIFT extracts a 41 \( \times \) 41 pixel patch at the given scale and rotates it to a canonical orientation. The patch is used to generate a compact feature vector by PCA (principle components analysis), which is then employed to construct a distinctive local descriptor for near-duplicate image matching. [17]

C. Distance Function in CBCD

- L1 and L2 distance function

Kim used L1 norm of Minkowski metric as the feature distance in [7]. L1 norm defined as follows:

Suppose two images X and Y are represented by p dimensional feature vectors \((x_1, x_2, \ldots, x_p)\) and \((y_1, y_2, \ldots, y_p)\), respectively.

\[
\Delta d_{ij} = |x_i - y_i|, \quad i = 1, 2, \ldots, p
\]

When \( r = 1 \), the above distance is the City-block distance or L1 distance. When \( r = 2 \), it is Euclidean distance function or L2.

- Dynamic partial function

In [28] and [29], a dynamic partial function (DPF) was proposed for discovering a better perceptual distance function through mining a large set of visual data. Meng et al. [30] developed an enhanced DPF to solve the “one-size-fits-all” problem in DPF. Meng et al. [31] applied DPF to image copy detection.

The dynamic partial distance function is defined as Eq.5, \( \Delta d_{ij} = \text{The smallest m } \Delta d's \text{ of } (\Delta d_1, \Delta d_2, \ldots, \Delta d_p) \)

m and r are two tunable parameters. The DPF can cluster similar images more compactly and keeps dissimilar images away based on a proper m value. The training dataset is employed to predict the optimal m value.

They employ a multi-resolution image representation scheme and represent each image as a 240- dimensional feature vector, which includes three types of perceptual features: color, texture and shape. Their experimental results show that by using texture features obtained from both Gabor filter bank and Wavelet filters, the system can reach higher accuracy than by using one of them alone.

IV. NEW TECHNIQUES APPLIED IN CBCD

A. Media Hashing Applied in CBCD

Media hashing is another method of content identification and copy detection. In contrast to data hiding, the main characteristic of media hashing is its non-invasive property, which means that no information has to be embedded in the digital content. On the other hand, a hash sequence for specific media data needs to be extracted to obtain a condensed representation. The major feature that distinguishes media
Venkatesan et al. [33] proposed an image hash function that converts the traditional hash function to a valid one for copy detection. Their algorithm, which uses randomized signal processing strategies to compress images into random binary strings in a nonreversible way, has been shown to be robust against some image changes.

In [34], Mihcak et al. used iterative geometric techniques that can tolerate geometric distortion in images. By so doing, their algorithm can withstand slight geometric distortions. Recently, Lu et al. [35] proposed a geometry-invariant image hashing scheme that uses mesh-based hash extraction and hash matching for similarity measurement. The proposed method can handle geometric attacks better than conventional media hash techniques. It is worth noting that, although media hashing originated from cryptography, it can still be viewed as a method of discovering a robust feature vector in an image that can tolerate errors caused by attacks. [17]

### B. Extended Feature Sets Applied in CBCD

The accuracy of the copy detector depends to a large extent on the robustness of the feature, and on a suitable threshold that can balance false rejection and false acceptance rates. However, although features with possibly high identification power have been introduced, they may not be effective under various kinds of attacks. This reflects a limitation of previous approaches: they lack the ability to exploit useful prior information, such as possible attack models, to improve copy detection performance. The limitation makes these approaches vulnerable to malicious attacks. Figure 3 illustrates this phenomenon. I denote the feature vector of a copyrighted image, A and B be the vectors obtained by applying some attacks to the copyrighted image, and C be an unrelated feature vector. The radius of the cluster $\epsilon$ denotes the error tolerance for finding copies in the feature space. In practice, an attack on a feature, say A, can often be successfully resisted, but attack on some other feature, such as B cannot be detected if it is far away from I in the feature space. Increasing the threshold of the acceptance range $\epsilon$ could detect the attacked image B, but C could be wrongly detected as a copyrighted image.

Hsiao et al. proposed an approach to image copy detection based on extended feature sets (EFS). Figure 4 illustrates the concept of using EFS to enhance the performance of copy detection, where the gray points are the extended features generated from prior simulated virtual attacks. The boundary between the copyrighted image and unrelated images can be defined more precisely by learning a classifier; thus, the copy detection problem can be solved more effectively. [17] Hsiao et al.’s algorithm [17] is summarized as follows:

1. chooses the DCT ordinal feature proposed in [7] and the extended futures to build the feature space.

2. Use three pattern classification methods that are the multivariate Gaussian, the Gaussian mixture model (GMM), and the support vector machine (SVM) to learn the copy detectors.

3. The trained multivariate Gaussian classifier is applied to test images in the first stage as it is faster for classification.

4. The more effective classifier, SVM or GMM, is applied to test images in the second stage.

The precision/recall-breakpoint (BEP) point is the point where the precision and recall are equal (or very close) in the PR curve. BEP has been widely used as a performance measure in classification problems. Table 2 shows the BEP of various detect methods. The experimental results show that Multivariate Gaussian framework based on EFS achieves a better performance in terms of BEP than the DCT ordinal measure, but the average detection time increases slightly.

### V. CONCLUSIONS AND DISCUSSION

We reviewed various kinds of image copy detection techniques on above sections. Obviously the developments of these techniques are followed by two main directions: one is digital watermarking, another is CBCD.

Digital watermarking developed from spatial domain to transform domain, from DCT to wavelets transform. In practice, although many techniques have been proposed, watermark-based frameworks still suffer from robustness problems; consequently, malicious users could remove a watermark via post processing.
The DCT ordinal feature is particularly suitable for efficient image copy detection over the Internet, since it can be applied to compressed image formats (such as JPEG). However, a limitation of the features generated by the ordinal measure is that they are not robust against geometric attacks.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their comments which have led to improvements of this paper. This work is supported by Zhejiang Province NSF Grant # Y106332.

REFERENCES


[27] Ming-Ni Wu, Chia-Chen Lin, Chin-Chen Chang, A Robust Content-Based Copy Detection Scheme, Fundamenta Informaticae 71 (2006) 351–366, IOS Press


