Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.99 – 105

RESEARCH ARTICLE

Video Forgery Detection Using Invariance of Color Correlation

Sarah Joy, Lisha Kurian

M-Tech Student, Sree Narayana Gurukulam College of Engineering and Technology, Kerala

Asst. Prof, Sree Narayana Gurukulam College of Engineering and Technology, Kerala
sarahjoy5989@gmail.com, lishakurian@gmail.com

Abstract- Video forgery detection aims to trace a query video snip in a video file or database. It helps in detecting video copies for copyright protection and reduces storage redundancies. In this paper, we put forward an effective method based on the invariance of color correlation. The proposed technique first split each key-framework into nonoverlapping block For each block, the red, green, and blue color components are sorted according to their typical intensities, and make use of the percentage of the color correlation to build a frame feature with a minimum size. Finally, the ensuing video feature is made up of the successive frame features, which is verified to be robust beside most typical video content-preserving operations, together with geometric deformation, blurring, noise infectivity, contrast augmentation, and strong re-encoding. The investigational results show that the projected method outperforms the accessible methods in the literature, as sound as the system based on the traditional color histogram.

Index Terms— Color correlation, content-based technology, video forgery detection, histogram analysis, video sequence matching

I. INTRODUCTION

Video may be modified by various techniques so that these customized videos may be used without the permission of the actual owners. This happens sometimes in sensor boards. In order to detect these forged videos we propose a modern technique based on the invariance of color correlation. Here each video sequences are divided into frames. Then we sort these frames based upon the intensities of RGB components and draw histograms accordingly. Here we use the color correlation algorithm to plot the histograms. Nowadays it is very common to find copies of the same video frames in the internet. This leads to wastage of data storage. By removing the detected copies we shall save space. Our proposed system also targets these kinds of problems also. The proposed system finds the copies of video frames using the video sequence matching. Forgery detection and video sequence matching go hand in hand with the color correlation algorithm.

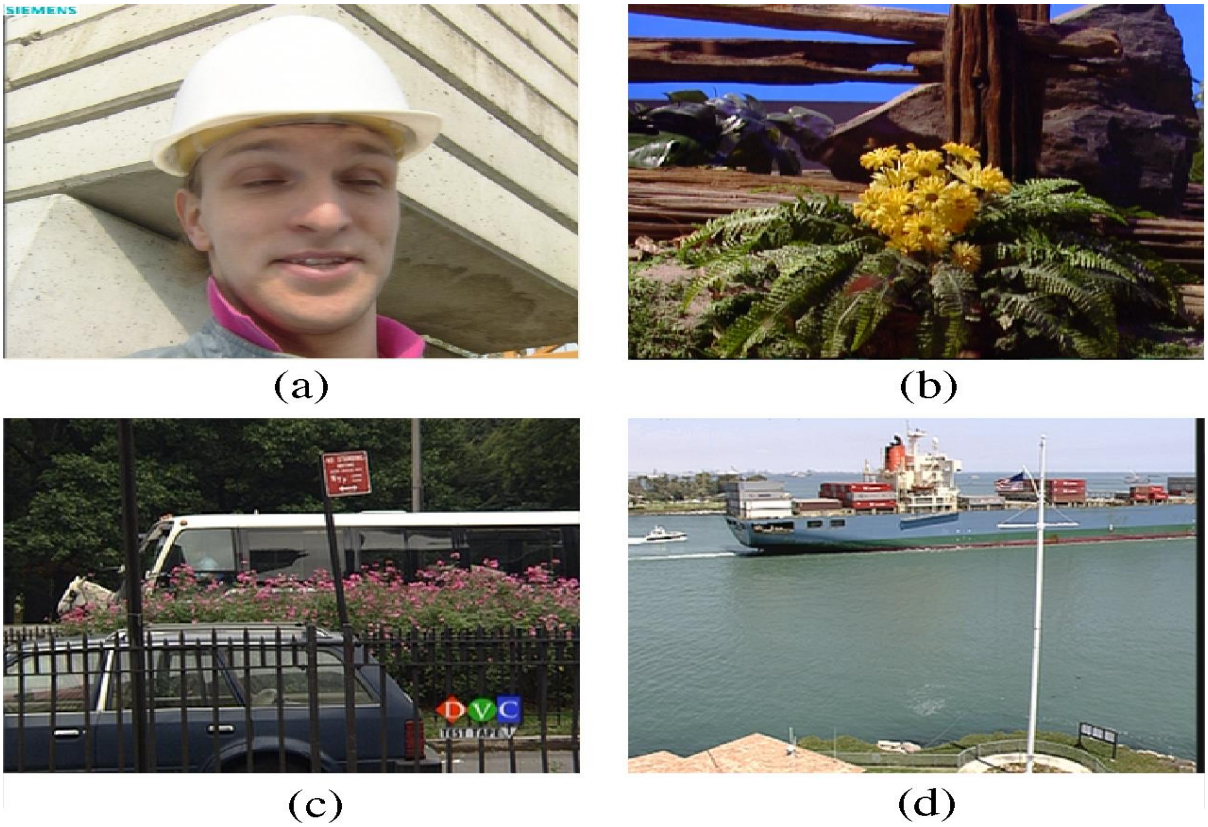

Fig1:Four distinctive videos. (a) *Foreman*. (b) *Tempete*. (c) *motor vehicle*. (d)ship.

II. SYSTEM OVERVIEW

Video forgery detection can be accomplished only through the systematic functioning of the various subsystems. The proposed system is very typical since it has a well organised feature extraction technical gadget that performs the best extractional operation of the sorted frames. Sequences of the various key frames are matched with the features extracted from the original videos. If there exist any similarities between the frame features then the query video is confirmed to be a forged one. It is not necessary that the query video is the exact copy of the original video; the modified original videos are also considered to be forged sequences. Certain content preserving operations such as rotation, scaling, flipping, letter box, pillar box, cropping, shifting, insertion of patterns, picture in picture, Gaussian filtering, average filtering, median filtering, motion blurring, Gaussian noise, histogram equalization, gamma correction, re-encoding may be done to the original video. These types of operations will preserve the contents as such but will have small modifications. These videos are also detected as forged ones by the proposed method.

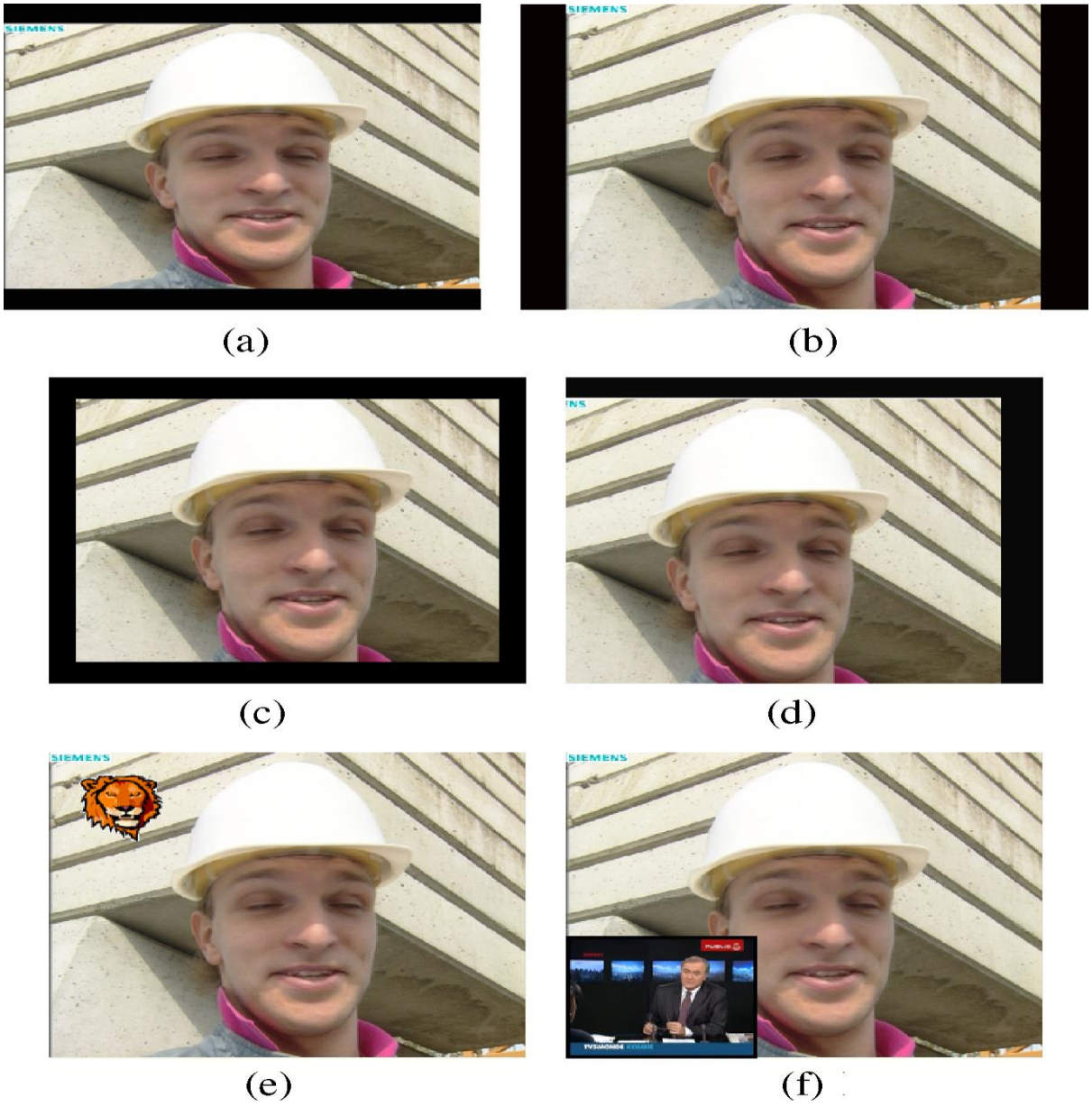

Fig2:Modifications done to the foreman video;
(a) Letter box. (b) Pillar box.(c) Cropping. (d) Shifting. (e) Picture insertion. (f) Video in video

A. SPLITTING OF VIDEO SEQUENCES INTO VIDEO FRAMES

The primary step in the proposed system is the splitting of the video sequences into key frames. A video may be composed of thousands of frames. The feature extractions of the video may be done only after converting the video into the frames. This will also reduce the complexity of the processing. Video frames may then be kept into observation to study about the nature and contents of the video. The average block intensity of the video is estimated. According to this estimation the video may be divided into various frames. Each frames may consists of sub images and all the images in the selected frame may be screened perfectly. This kind of evaluation of images will definitely help in the detection of forged videos. Similar images or videos are examined in order to confirm any forgeries. Video content identification is carried out in this phase. Therefore splitting of video into corresponding video frame is of great importance.

B. SORTING OF FRAMES BASED ON COLOR INTENSITIES

The key frames are sorted according to their variation in RGB values or intensities. This RGB components of each frame is calculated and frames of similar intensities are put together. There are six constraints, they are

a) $R_{xy} \geq G_{xy} \geq B_{xy}$

b) $R_{xy} \geq B_{xy} \geq G_{xy}$

c) $G_{xy} \geq R_{xy} \geq B_{xy}$

d) $G_{xy} \geq B_{xy} \geq R_{xy}$

e) $B_{xy} \geq R_{xy} \geq G_{xy}$

f) $B_{xy} \geq G_{xy} \geq R_{xy}$, where $1 \leq x \leq w$, $1 \leq y \leq h$

Based on these constraints the frames are sorted. These six conditions are checked for every frames. Every frames will be placed in one of these constraints. The sorted frames are then send for feature extraction.

C. FEATURE EXTRACTION

The sorted frames are screened one by one and their features are extracted .Color transformation of the various frames are noticed and they are recorded. The extracted features are represented in feature bits. This step by step process is demonstrated in Fig 1.

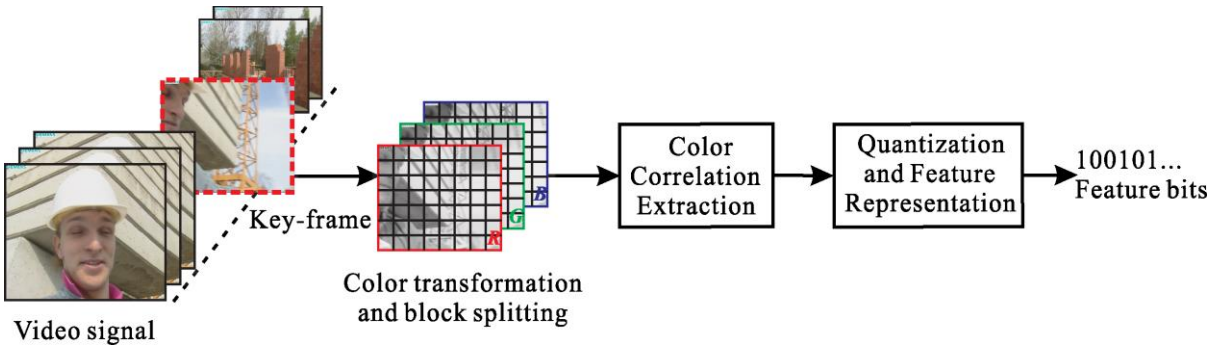

Fig 3:Feature extraction of a video sequence

Quantization of the color correlation is a time consuming process. This may vary according to the complexity of the video sequence. Feature bits are binary in nature. Block splitting can sometimes lead to destruction of frames.

D. PLOTING HISTOGRAMS

After extracting the features, the next step is to plot histogram based on the features. Feature bits are screened to plot the histograms. This is for the easy analysis of the video content. Using the ploted histograms one can very easily find the intensities of color components. Histogram is a pictorial graph representation of the extracted feature bits. The ploted histograms are then analysed to compare the features of various frames.

E. HISTOGRAM ANALYSIS

Analysis of the histogram will be helpful to compare the features of one frame with another. The histograms for the four distinctive videos are as follows.

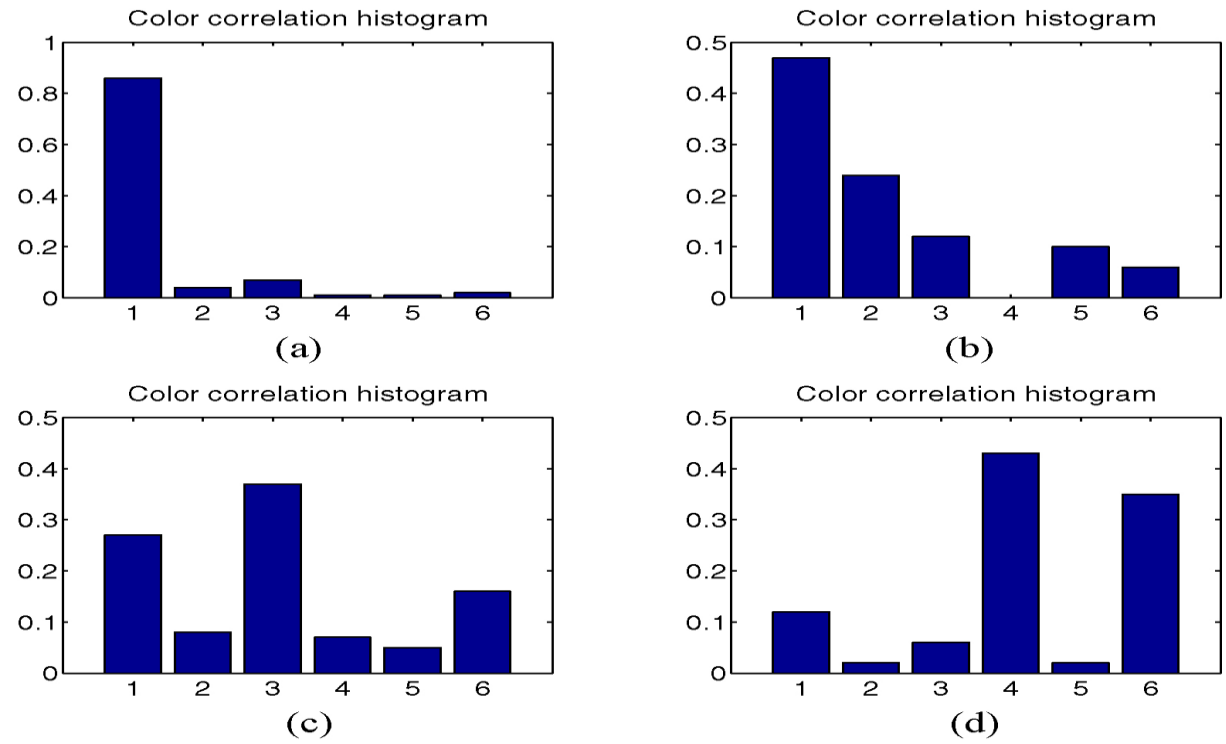

Fig4:Histograms plotting color correlation of the distinctive videos

F. FORGERY DETECTION

The proposed system detects not only the exact copies but it also analyse the modified videos. Therefore this system is highly efficient. The detection of the forged video is done with the help of color correlation algorithm that is described below.

COLOR CORRELATION ALGORITHM

Step 1:Extract the frames from video sequence.

Video *V* is assumed to be composed of successive *N* key-frames, denoted by *V* =_*V*1, *V*2, ・ ・ ・ , *VN*_, so that the features of the video can be denoted as follows.

HV =_*HV*1,*HV*2 , ・ ・ ・,*HVN*,where *HVi* denotes the color correlation feature of the video frame *Vi*, and *i* = 1, 2, ...,*N*.

Let *Vq* and *Vt* be two different videos with *N* key-frames.

Step 2: The space between the two different videos is defined as the middling of the space flanked by the corresponding key frames .

d(*HVq, HVt*) =*N_Nk*=1

d(*HVq,k, HVt,k*) where *HVq,k* and *HVt,k* are the color correlation of the *k*th frame in the videos *Vq* and *Vt* .

Step 3:Extraction of features of each of the key frames.

_6∑

i=1*H*(*i*) = 1 0 ≤ *H*(*i*) ≤ 1 *i* = 1, 2, ..., 6,*where H(i) is any real number. Also if there is two distinct features Hq(i)and Ht(i) then the space in between them is calculated using the following equation*

$d(H_q,H_t) = 1/C\_6\sum_{i=1} |H_q(i) - H_t(i)|$.

Step 4:Plot histograms based on the color intensities of the features extracted.

The normalized histogram can be represented based on the following formula where|*Pi*| is the cardinality of set *Pi*

H(*i*) =|*Pi*|_6∑*i*=1|*Pi*|

Step 5:Detection of forged videos by analyzing the modifications done to the original video sequence.

Hm(i) =3/c∑i=1 |pj|/|pi|

Pi = {(˜*Rxy, ˜Gxy, ˜Bxy*)|˜*Rxy, ˜Gxy, ˜Bxy*,where Hm(i) is the forged frame.

III.PERFORMANCE EVALUVATION

In this experiment, the efficiency of the proposed scheme evaluate on a video dataset and over 4000 query clips with various commonly-used transformation. Here we further evaluate the performances of different schemes using the MUSCLE VCD benchmark .This publicly available benchmark provides a database and there are two different tasks. For the first task, there are totally 15 query clips, and it aims to find the corresponding near-duplicates of entire query videos in the database. For the second task, there are totally three queries that are generated as follows: six to eight short subsequences extracted from different videos in the database are inserted into a video that is not in the database.

The performance degree used for video forgery detection, which is easier to express than for localization and extraction, is the detection rate, defined as the ratio between the number of detected video key frames and all the given frames containing the modifications. Measuring the performance of frame extraction is enormously difficult and until now there has been no comparison of the different extraction methods. Instead, the performance is merely inferred from the existing results, as the feature extraction performance is closely related to the desired output. Traditionally in evaluation of video forgery detection algorithms, for a single detection file and its corresponding ground truth file, two values, recall and precision, can be calculated. They are defined as follows:

$$Recall = \frac{correct\ Detected}{(Correct\ Detected + modified\ \ video\ frames)}$$

$$\text{Precision}=\frac{Correct\ Detected}{(Correct\ Detected + False\ Positives)}$$

TIME COMPLEXITY EVALUATION

Here, we for the most part inspect the computational outlay of the feature extraction. In this experiment, we dash all the algorithms in the identical environment. It must be supposed to be renowned that there are no equivalent operations. Table summarizes the average consumed time over 5000 s record for all the algorithms to extract a frame attributes. It is evidently pragmatic that SOM(spatial ordinal measurement) and TOM(Temporal ordinal measurement) perform the fastest, and the SIFT-based approaches are the slowest. For the proposed scheme, it takes an average of 9.434 ms to achieve the feature extraction for a frame, which can convince the necessities of real-time application.

SPACE COMPLEXITY EVALUATION

SOM employs the position of standard intensities of four blocks as a feature, whose value is in the set of *{*1, 2, 3, 4*}*.Thus, each outline can be represented by 4 × 2 = 8 bits. If an analogous technique is used, we can further condense the 8 bits to (4−1)×2 = 6 bits. TOM stores the typical intensities of four blocks, thus 4 × 8 = 32 bits are needed. With quantization and compression technique, each group of five successive elements is encoded into 8 bits, thus 160 bits are required. For the SIFT-based schemes, descriptors are quantized into 200 visual terms. As described previously, our proposed scheme requires 35 bits. Based on Table, it is practical that the most excellent method, in terms of storage, is SOM, requiring the most storage.

Compared with the original version , the resulting videos would appear quite diverse from the original ones, and become very artificial after these operations. In such cases, the color correlations among the red, green, and blue components are significantly altered, meaning that the proposed feature will be unsuccessful. However, for the other 11 videos with some complex transformations, our proposed scheme can still successfully work.

Table 1: TIME AND SPACE COMPLEXITY OF THE ALGORITHM.

Methods	Execution Time (ms)	Required Storage (bits)
SOM	4.87	8
TOM	4.69	37
SIFT	220.25	1500

Table 2: EXPERIMENTAL RESULT OF THE ALGORITHM.

#videos	200
# forgeries	35
#correct detected	164
#false positives	12
Recall (%)	82.30%
Precision (%)	89.70%

IV. CONCLUSION

This proposed system is a new video forgery detection system that detects and recognizes forged video sequences from an original video database. In this paper Color correlation algorithm is proposed to overcome the difficulties of grouping the characters and remove false positives. The proposed system compares favorably with the existing algorithms when handling complex videos and achieves significantly enhanced performance in complex natural scenes and also blurred edited sequences.

ACKNOWLEDGEMENT

The authors would like to thank the Associate Editor and the anonymous reviewers for their valuable comments, also special thanks to Lei and Luo for their help on the Correlation method.

REFERENCES

[1] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proc.IEEE, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.

[2] Y. Li and R. H. Deng, "Publicly verifiable ownership protection for relational databases," in Proc. ACM Symp. Inform. Comput. Commun.Security, 2006, pp. 78–89.

[3] X. Kang, J. Huang, and W. Zeng, "Efficient general print-scanning resilient data hiding based on uniform log-polar mapping," IEEE Trans.Inf. Forensics Security, vol. 5, no. 1, pp. 1–12, Mar. 2010.

[4] A. Joly, O. Buisson, and C. Frelicot, "Content-based copy retrieval using distortion-based probabilistic similarity search," IEEE Trans. Multimedia,vol. 9, no. 2, pp. 293–306, Feb. 2007.

[5] E. Chang, J. Wang, C. Li, and G. Wiederhold, "RIME: A replicated image detector for the world-wide web," Proc. SPIE Multimedia Storage Archiv. Syst., vol. 3527, pp. 58–67, Nov. 1998.

[6] C. Kim, "Content-based image copy detection," Signal Process.: Image Commun., vol. 18, no. 3, pp. 169–184, Mar. 2003.

[7] M.-N. Wu, C.-C. Lin, and C.-C. Chang, "Novel image copy detection with rotating tolerance," J. Syst. Soft., vol. 80, no. 7, pp. 1057–1069,Feb. 2007.

[8] J.-H. Hsiao, C.-S. Chen, L.-F. Chien, and M.-S. Chen, "A new approach to image copy detection based on extended feature sets," IEEE Trans.Image Process., vol. 16, no. 8, pp. 2069–2079, Aug. 2007.

[9] A. Qamra, Y. Meng, and E. Y. Chang, "Enhanced perceptual distance functions and indexing for image replica recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 3, pp. 379–391,Mar. 2005.

[10] Z. Xu, H. Ling, F. Zou, Z. Lu, and P. Li, "Robust image copy detection using multi-resolution histogram," in Proc. ACM Int. Conf. Multimedia Inform. Retriev., Mar. 2010, pp. 129–136.

