Image Authentication – A Content Based Technique

Manasa S.
6th SEM
Dept. of ISE
City Engineering College
ranimanasaiyer@gmail.com

Greeshma G.
6th SEM
Dept. of ISE
City Engineering College
greeshmanju@gmail.com

Abstract

This paper is focused on image authentication, as the process of evaluatingthe integrity of image contents relatively to the original picture and of being able to detect, in an automatic way, malevolent image modifications. The paper begins with the description of a general framework for content based authentication of images and video. Then, a specific method is proposed. It relies on image edges and tries to tackle the problem of hagelvideo integrity from a semantic, high-level point of view. Experimental results are presented for well-known image and video sequences.

Index- image authentication, content based technique, image edges, image extraction.

1. Introduction

The emerging and the foreseen growth of digital multimedia works together with the intrinsic capability of such media to be copied, manipulated and transformed. Requires new protection schemes to be developed. This paper is focused on imageauthentication, as the process of evaluating the integrity of image contents; relatively to the original picture, and of being able to detect, in an automatic way, malevolent image modifications. Being impossible, in most situations, to access the original work to perform this,kind of verification, a possible solution is to associate to the image some additionalinformation (or *Iuhel)* linked with (i.e., dependent on) the picture content. To beeffective, this label should identify, in a (quasi) univocal way, an image or video sequence. The label can assume the form of an header juxtaposed to the picture, orit can he written on a different medium and indexed by a pointer conveyed with thepicture (inlayed on it using watermarking techniques, or as a small header). Forvideos, the label shall apply on each image individually, and labels of differentframes should be linked together in order to assure the video integrity.

In order to link the label content with the picture content, two different approaches can be followed:

A pure mathematical solution by which a hashing function is found, with such properties that, when applied to two different bit-streams (in the limit differingby only one bit) results in two different bit sequences (with ***a*** length muchshorter than the original bit-stream).

To extract, at the image Icvel, essential image characteristics that should survive the whole processing and transmission chain (creation, production, mnp5; session and broadcasting), The first approach should be used when strict image integrity is required and nomodification is allowed. It can be considered a classical problem for which cryptologists already have some solutions [I]. The second approach has to be usedwhen regular image manipulation (e.g. compression, colour space transformation, gamma correction, contrast modification) is admitted, but irregular manipulation (E.g. logo insertion, objects deletion, objects modification) must be detected.

Here we are concerned with the second case, for which image related information (here after designated by *image features),* have to be extracted.

2. A Generic Structure for Image Authentication

Figure 1 presents main elements and their interactions of a generic structure for image authentication.

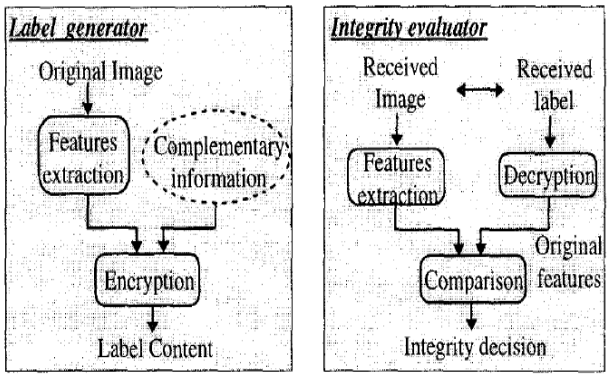

Figure 1: A Generic Structure for Image Authentication

Feature extraction

In order to assure image integrity, main requirements for the extracted image features are:

* Univocally identify the image (or video sequence) Invariance under mild (barely perceivable) compression.
* Sensitivity (i.e., not invariant) to modifications such as compression abovevisibility threshold, geometric transformations (rotation, translation andzooming), etc.

High sensitivity to contents manipulation, with emphasis on logo insertion and objects deletion/insertion. Real-time computable, using low-cost and existing technology. Depending on the specifications for label size, this block may also include acompression stage.

Complimentary information

Generic information about the picture and itsauthor, e.g., image identification number (IIN), assigned by an author society toeach original work, which may serve as a pointer to a database where the wholecopyright information is contained or where the image features will be stored. Itran alcn he useful to rights management's if it permits identification [2].

Encryption and **Decryption**

In order to assure that the label contents (i.e., image features + complementary information) cannot be faked, all this informationmust be signed by a private key. Associated with this private key, there is a publickey, known and used by the authentication system (or"integrity evaluator" infigure I), to decrypt the label.

Comparison

Features extracted from the image for which authentication has tobe evaluated ("received image" in figure **1.)**Are compared with the featuresconveyed in the associated label. The key element in this block is a similaritymeasure between extracted and original features that should differentiate errorsdue to authorized modifications from errors due to malevolent manipulations(necessary i l truly invariant features cannot be obtained).

3. Authentication Based On Image Edges

Image authentication schemes will differ in the particular implementation of the *"Features extraction"* and *"comparison"* blocks of figure 1: in *[3]*, the extractedfeatures are block-based image infinity histograms and means, and the Euclidemdistance was used as similarity measure; in [4], the relationship between pairs ofDCT coefficients of the same position in separate blocks of the image, translated toa binary sequence, is used as features; in the authenticator, a mere comparisonbetween two binary sequences (original andcomputed from received image) isperformed. In this section we propose an algorithm for image authentication basedon image edges.

We should be aware that edges (its position and value) can be modified if high compression ratios are used and that the success of this kind of approach is greatlydependent on the capacity of the authenticator system, to discriminate betweendifferences in the edges due to compression from those due to semantic imagemodifications.

4. Algorithm Structure

Figure 2 presents the block diagram of the proposed features extraction andintegrity checking systems.

Features extraction

To obtain a binary image marking edges and no-edges pixels the gradient, computed at each pixel position with the Nobel operator, iscompared with a threshold obtained from the gradient histogram *[5]*. Better edgesrendition could be obtained using the Canny edge detector (with the advantage ofbeing less sensitive *to* additional image noise), but at the expense of a highercomputational cost.

The resulting bit-map is then compressed. Depending on the specifications forlabel size, the bit-map could be firstly submitted to a lossy compression schemewith the propose of reducing its spatial resolution *("sub-sampling"* in figure 2).

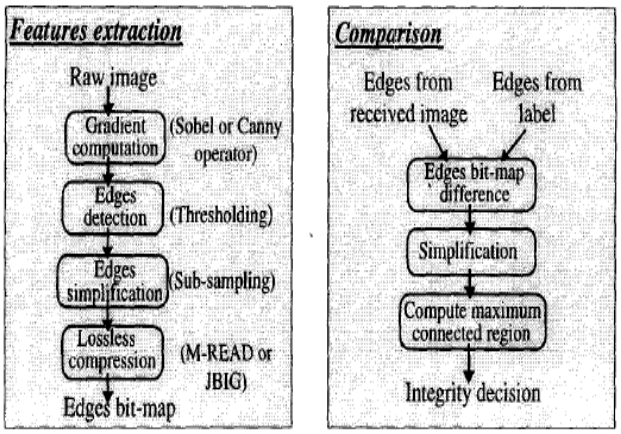

Figure 2: Algorithm structure

A simple majority filter or the technique proposed in the JBIG standard can beused and have been implemented. Finally, the edges bit-map is entropy encoded. Here, two lossless compression techniques for binary images can also beenvisaged: Modified READ or JBIG.

Comparison between original and extracted features

Most of the currentlyavailable compression techniques (those based on frequency analysis, like DCT orsub-band) tend to distort contours. When DCT coding is applied to a block thatcontains an edge, two types of distortion appears: i) the quantization of the DCTcoefficients cause the smoothing of the edge; ii) the use of a separableimplementation of the DCT results is an ambiguity in the orientation of the edge,which causes the appearance of an edge in the direction perpendicular of the actualone *("mosquito noise")* [6]. This kind ***of*** errors should be used **as** *prior knowledge*by the authenticator system.

Referring to figure 2, the "edges bit-map difference" block provides two types ofoutputs: 1) a binary mask marking error pixels (pixels where there is a differencebetween original and computed edges bit-maps); ***2)*** a confidence measureassociated with each error pixel and where the above mentioned *prior knowledge*about compression errors is introduced. In the "simplification" block and for eacherror pixel, a *context* is then evaluated. Depending on its context, the confidence ofthe error **is** modified. These two procedures - context evaluation and certitudemodification (similar to *edge relaxation*procedures) - was implemented in a verysimplified manner (truly relaxation procedures could be very computationallydemanding):

i) Confidence measure

for each error pixel, a certitude was computed as a function of the distance between the gradient at that pixel position and the edge no edge decision threshold (in fact, the smaller the distance is the less certain the decision will be), and also as a function of the spatial distance from that error position to a good matching position (in this way, the errors due to the mosquito noise will receive a low certitude value). After that, all the confidences are compared with a predefined value, resulting in a binary decision (low or high certitude) for each error pixel.

ii) Error relaxation

(Or "simplification" in figure 2): low certitude errors arecompared with their neighbor's (in a second order neighborhood) - if at least 3 ofthe neighbors are high certitude errors, the certitude of the error is modified tohigh; otherwise it is maintained i n low. The procedure is iteratively repeated a11over the image until no more changes occur. At the end, all high certitude errors

Are considered to be true errors (and assigned a '1' in the error image) and lowcertitude errors are eliminated (a d assigned a '0' in the error image). Integrity violation is decided if, after simplification, the maximum connectedregion in the error image exceeds a pre-defined threshold (the optimal value fixthis threshold has to be determined in a statistical base, after further tests, usingdifferent compression rates and different kinds of manipulations).

Furthermore, in the case of video, i f a malevolent modification has taken place, itis expected that the temporal correlation of the errors should be higher than if theerrors are due to compression. This suggests a further level of integrity evaluationthat checks if the errors occur in the same positions for consecutive images. Due tomotion, all these correlations must be performed after motion compensation. Thiscan be included in the authentication scheme without increasing its cost, as motioncompensation already exists in the video decoder. Also, motion vectors are carriedin the video bit-stream, so they do not have to be computed.

5. EXPERIMENTAL RESULTS

Sensitivity to content modification

In order to evaluate the sensitivity of theproposed method to semantic content modification, the very well known*"Cameraman"* still image and *"Mobile and Calendar"* video sequence were used.

In the first one, the camera lens ***W, BS*** modified (the original picture can be seen infigure 3-a) and the modified one in figure 3-b)) and the resulting image

wascompressed (JPEG, with a quality factor of 50 %); in the second one, two smallobjects were manually deleted in the first ten frames. Figures 3-c) and 3-d) present, respectively, the error images (obtained **in** the"comparison" block of figure) after mere difference between received (in the label) and extracted edges bit-map, and1 the same difference after simplification, for***"Cunzeraman".*** In figure 3-c), the small and sparse errors are due to compression.

They are eliminated by the "simplification" block, and only the error regionresulting from the true manipulation appears at the integrity evaluator output. Themanipulation results in a connected region with a size much higher than those dueto compression errors, **and** is easily detected.

For "Mobile *and Calendar"* the results are similar. In this **case, the** manipulation(objects deletion) has been detected not only checking the integrity frame by frame,but also computing the temporal correlation of the error images for consecutiveframes.

Figure 3: "Cameraman" - a) Original; b) Manipulated and compressed with JPEG, Q=50%; c) Difference between edges bit-map extracted from a) and b); d) Difference after simplification (edges bit-map have been sub-sampled by a factorof 2 in horizontal and vertical directions)

Resistance to MPEG-2 compression

In order to evaluate the invariance of theextracted features with compression, tests were performed using *"Mobile* & *Calendar"* and *"Flower* &*Garden"* sequences, compressed using the MPEG-2standard at **6** Mbit /s and 4 Mbit/s. In this case, although the maximum connectedregion for the error images could attain significant values in some frames (usuallythe B frames at 4 Mbit/s) that are, in any case, smaller than those due to thesimulated manipulations, the temporal correlation of these errors is quite small(near zero if three consecutive frames are considered).

CONCLUSIONS

In this paper we have presented a generic structure of an image authenticationsystem and a particular implementation of that system, based on image edges. Taking into account the results obtained with first simulations and that imageintegrity should be evaluated on a semantic level, using image features with highperceptual significance, as edges are, the proposed technique can be considered avalid candidate for image authentication. Further tests are still needed in order tobetter qualify the approach and to better tune the involved parameters. This topic isthe subject of current work.

References

[l] B. Macq and J.J. Quisquater, "Cryptology for digital TV broadcasting '0 *PI-oc. of* ***the***

[2] J.-F. Delaigle *et al.,* "Digital images protection techniques in a broadcast framework: an

[3] M. Schneider and S.F. Chang, "A robust content based digital signature for image

[4] C. Lin and S.F. Chang, "A robust image authentication method surviving JPEG lossy

ISI N. Otsu, **"A** threshold selection method from grey-level histogram", IEEE Transactions

[6] C. Lambrecht, "Perceptual models and architectures tor video coding applications",

IEEE, ~01.83N, o.6, pp. 944-957, June 1995overview", Proc. ECMAST-96, pp. 71 1-727, Belgium, Miay 1996authentication", **Proc.** ICIP-96, **pp.** ***227-230***compression", Proc. **IS&T/SPIE,** January 1998on SMC, SMC-8, 1978, pp. 62-66

PhD Thesis no. 1520, EPFL, 1996