A Robust Hashing of ID Photos

Andreea Smoaca∗†, Mihai Petrovici† Daniela Coltuc† and Vasile Lazarescu†
†Politehnica University of Bucharest
Faculty of Electronics, Telecommunications and Information Technology, Bd. Iuliu Maniu 1-3, Romania
∗ Université de Lyon / CNRS, UMR 5516, Laboratoire Hubert Curien
Université de Saint-Etienne, Jean Monnet
Email:andreea.smoaca@univ-st-etienne.fr, mihai.petrovici@hotmail.com, daniela.coltuc@upb.ro, vl@elia.pub.ro

Abstract— The paper proposes an image hashing method that is highly robust to a series of currently encountered attacks on digital images. It is dedicated to images representing ID photos. The extraction of hash value is based on a global method for face recognition. Such approaches need a registration stage which is often obtained by means of face characteristic points. The detection of the characteristic points easily fails in the case of attacks like filtering, noise addition, random line deletion orandin compression, mainly when they overcome certain limits. Our solution is to attach the characteristic points to the final hash, in order to obtain increased robustness to such attacks. The final hash is obtained by stabilizing an intermediary hash extracted by using Independent Component Analysis. The stabilization is done by clustering. The final hash is given by the cluster label having attached the coordinates of three characteristic points.

We show that intermediate hashes of the attacked image approximate a hyper-sphere centered on the original image hash. Due to this fact, the minimization of a cost function representing the proximity to original hashes is sufficient to stabilize the intermediate hashes.

We also evaluate the system capacity by estimating the number of freedom degrees for the intermediate hashes of the non-attacked ID photos.

I. INTRODUCTION

A robust hash of a media file, such as an image, is a short binary representation of the most relevant perceptual attributes of the media. The hash is sometimes called digital signature, fingerprint, message digest or label. An essential requirement of image hash is the robustness, meaning that perceptually similar images should map to the same hash, even if they have different digital representation. A series of common processing, like jpg compression, filtering, noise addition or geometric modifications (crop, rotation, shift etc.) generates such images. They are called with the generic name of non malicious attacks. The hash should be robust to non malicious attacks, but sensitive to tampered or different images.

The robust hash is used in image authentication or for indexing large databases of images. Hashing is different from watermarking - another technique for media authentication - in that the hash is appended and not inserted in the image.

Robust hashing supposes two steps:

• Extraction of image features and assembling of an intermediate hash. The intermediate hash is a binary string of fixed length that is sensitive to attacks.

• Stabilization of the intermediate hash such to obtain a hash that is invariant to image non malicious attacks.

Feature extraction is often inspired from recognition methods. In the case of human faces, basic approaches that do not suppose pose changes or aging may be used, since the robust hashing is authenticating the image and not the person.

Popular face recognition methods can be categorized as global and feature based approaches. Principal Component Analysis (PCA), Independent Component Analysis (ICA), Linear Discriminant Analysis (LDA) or Local Feature Analysis (LFA) are some examples of the former category. In image analysis, they use vector bases with various properties: statistically independent (ICA), uncorrelated (PCA), correlated based on eigen-face decomposition (LFA) or obtained by maximizing Fisher’s discriminant (LDA). Being sensitive to pose changes, these techniques are preferred for frontal view faces classification. The latter category is based on geometrical relations between local facial features, compensating thus for pose changes.

Our application regards the hashing of ID photos. The intermediate hash is extracted by using a global method based on ICA. By clustering the intermediate hashes resulted from common non malicious attacks, a robust hash is finally obtained for each ID photo. This hash is used for the authentication of digital ID photo.

II. OBTENTION OF INTERMEDIATE HASH

The global face recognition approach used for feature extraction is based on ICA Architecture I [1], which leads to localized feature vectors. The process is modeled by the following equation:

\[ x = A \cdot s \]  

(1)

In this approach, the faces from a training set (Fig. 1) are serialized and placed on the rows of matrix \( x \). The ICA algorithm learns the pseudo inverse matrix \( W = A^{-1} \) used to find statistically independent components of the images (face characteristics: nose, eyes, mouth, etc.), estimated by the rows of matrix \( s \) that are used as basis vectors. Thus, any face image (from a test set) may be represented as a linear combination of face characteristics.

The procedure to extract the intermediate hash of the ID photos has been extensively described in [4]. It consists of the following steps (Fig. 1):

a) Image preprocessing and registration, both for the training set and test set. The registration is done by means of eyes and mouth coordinates.
b) **Basis learning** by applying ICA on the training set in Architecture I configuration.

c) **Subspace selection** by discarding in PCA stage of ICA, the eigen vectors corresponding to the lowest eigen values.

d) **Obtention of** \( b_k \) **coefficients** by test faces decomposition onto the subspace vectors.

e) **Coefficients quantization and binarization.** Each \( b_k \) is uniformly quantized on \( L \) levels and converted to binary by a Gray code on \( \log_2 L \) bits.

The intermediate hash is obtained by concatenating the binarized coefficients \( b_k \). It has a bitlength of \( N \log_2 L \), where \( N \) is the selected subspace dimension.

The registration in the first step is done by using three characteristic points: the two pupils and the mouth center. Our analysis method is very sensitive to this step. A misregistration compromises the feature extraction. As the characteristic points detection is difficult on images attacked by lossy compression, filtering or noise, we append the points coordinates to the stabilized hash.

### III. INTERMEDIATE HASH STABILIZATION

Two approaches has been reported in the literature, for intermediate hash stabilization: channel decoding [5] and clustering [3].

Channel decoding has the disadvantage of using a predefined partition of intermediate hash space. This space has the dimension equal to the bit length of intermediate hash, which is \( N \log_2 L \) in the case of our method. The intermediate hashes of the attacked versions of an image constitute a cluster of points in this space. The cluster position depends on image content and on the extracted features. If the cluster is positioned on the frontiere of two partition regions, then robustness may be completely lost.

The clustering creates its own partition, which is adapted to existing intermediate hashes. The intermediate hashes are grouped in clusters by optimizing a cost function. A simple solution is to use as cost function the Hamming distance between the intermediate hashes to be clustered and those of the originals. Fig. 2 shows the histograms of genuine and impostor distances, in the case of jpg compression with quality factor 10. By genuine distances, we mean the Hamming distances between the original and attacked intermediate hashes and by impostors distances, the Hamming distances between hashes of different ID photos, either original or attacked. The histograms support shows that the hash of an attacked image is closer to the original’s hash than to hashes of other ID photos. Of course, if the attack is in certain limits.

We have tested two algorithms that minimize the distance to cluster centers: K-nearest neighbor and K-medoids, with Hamming distance. As initial centers, the algorithms have received the intermediate hashes of the originals. K-means

![Fig. 2. Normalized Hamming distance distribution. With black, genuine distances distribution and with gray, impostor distances distribution.](image)
refines iteratively the centers, while K-nearest neighbor preserves them. Once classified, an intermediate hash is stabilized to the cluster label.

The final hash is constituted by cluster label and the coordinates of the three characteristic points - eyes and mouth - used for image registration.

With K-medoids, each stabilization of an intermediate hash refines a cluster center. Since the stabilized hash is the cluster label, not its center, the new arrived intermediate hashes should not influence the stabilization, if the clusters are spherical.

We have evaluated the clusters form by looking at the distance distribution. More precisely, we have estimated the distance distribution on each axis of the selected subspace by counting the number of bit changes for some given attacks. The histogram obtained for 210 ID photos has shown a rather uniform distribution (Fig. 3), meaning approximately spherical clusters centered on the intermediate hashes of the originals.

With this assumption, K-medoids may be replaced by K-nearest neighbor, which is a simpler algorithm. Thus, each cluster is constituted by the closest points (intermediate hashes of the attacked images) to a given original intermediate hash.

The enrollment of a new ID photo is done by initiating a new cluster by its intermediate hash. A distance condition must be accomplished by the new ID photo hash: the Hamming distance to the registered hashes must be over a predefined threshold. We have estimated this threshold by modeling the Hamming distance histogram of the 210 ID photos, by a binomial distribution (Fig. 3), meaning approximately spherical clusters centered on the intermediate hashes of the originals.

Another aspect of hash stabilization by clustering is the label dimension in bits. The dimension is a tradeoff between two opposite demands:

- The final hash must be short (shortness is a desirable property for hashes, since hashes are attached to the image)
- The final hash must be enough long in order to have sufficient capacity for the verification system (database with the original intermediate hashes). For $n$ bits length labels, the system may receive, at most, $2^n$ hashes.

The maximum length may be obtained by estimating the number of freedom degrees of intermediate hashes. Since by our method, the intermediate hashes are not statistically independent, it is less than 360 bits. Indeed, the binomial modeling the Hamming distance distribution has shown only 100 degrees of freedom, meaning that the enrollment capacity of our system is of $2^{100}$, which is more than sufficient.

The disadvantage of clustering, by respect to channel decoding, is the need for a database, which archives the intermediate hashes of the originals.

IV. EXPERIMENTAL RESULTS

Our approach was tested on a subset of FERET database of facial images [6]. Only images of frontal view and neutral expression have been considered, in order to stay close to ID photo case. The training set used for learning the ICA basis vectors consisted of 300 gray level images of 384x256 pixels. For robustness tests, another set of 210 different subjects, with the same characteristics was considered.

All the images were normalized in order to have zero mean and variance equal to one, registered, cropped and resized to 60x50 pixels. The registration was done by using the eyes and mouth coordinates provided by FERET databases. By averaging the training images coordinates, a reference set of coordinates has been obtained. All the faces, for training or tests, were registered to the reference set.

A representation basis, consisting of 120 ICs, was learned by applying ICA (Architecture I) on the training set. By projecting the test images on this basis, a set of 120 coefficients was obtained for each image. The coefficients were uniformly quantized on 8 levels, binary encoded by Gray code and assembled in a 360 bits intermediate hash.

Each test image has been attacked by median filtering, jpg compression, additive white gaussian noise (AWGN), rotation, shifting, random lines deletion, affine transforms from Stirrmark benchmark and an intermediate hash has been extracted, each time, by the mentioned procedure. For registration, the original coordinates of eyes and mouth have been used since they are supposed to be known, being included in the hash attached to the image.

For stabilizing the intermediate hashes, we have tested clustering by K-nearest neighbor and K-medoids, with Hamming distance. The clusters have been intialized by the intermediate hashes of the non attacked images. The final hash is a cluster label represented on 100 bits (according to the binomial distribution in Fig. 4) having appended 3 pairs of coordinates. By representing a coordinate on 10 bits (images up to 1024x1024 bits), a final hash of 160 bits is obtained.

For clustering by K-medoids, 100% correct classification has been obtained for the following attacks:

- 15x15 median filtering.
- jpg compression with quality factor (Q) of 10 or higher.
- AWGN with $\sigma = 0.5$ or lower.
- rotation by up to 0.5 degree.
- random deletion of up to 3 lines.
- shifting by 2 pixels.
- affine transforms 1, 3 and 5 from Stirrmark attacks.

The robustness at median filtering is very high, comparing with other results reported in the literature ( [2], [3], [5]). This is explained by the including of registration points in the final hash and by feature extraction procedure. More precisely,
in the preprocessing step, the image resolution is reduced by resizing to 60x50 pixels and the image is projected on a selected set of ICs.

The robustness at jpg compression and AWGN is in normal limits. Fig. 5 shows an ID photo, attacked by 15x15 median filtering, jpg compression with $Q = 10$ and AWGN with $\sigma = 0.5$. Its final hash is not affected by these attacks.

The robustness to rotations, random lines deletion and shifting is reduced because our hashing is very sensitive to image registration. The results reported for other methods ([2], [3], [5]) are about 2 degrees for rotations and up to 5 lines for random deletion. Table I shows the percentage of correct classification, in the case of our hashing, for these levels. The little robustness that is however obtained is due to the resizing in the preprocessing step that reduces the image size by 2. An increased robustness to these attacks could be obtained by using higher resolution ID photos or by allowing some freedom in registration.

The use of K-medoids instead of K-nearest neighbors for clustering gives worse results. The final hashes are robust only up the following attack levels:

- 11x11 median filtering.
- jpg compression with $Q = 10$ or higher.
- AWGN with $\sigma = 0.3$ or lower.
- rotation by up to 0.25 degree.
- random deletion of a single line.
- shifting by 1 pixel.
- affine transforms 1 and 3 from Stirnmark attacks.

We have estimated the cluster centers for three attacks with various levels of intensity: jpg compression, median filtering and AWGN. The cluster centers obtained for jpg compression, median filtering and AWGN differ from the K-nearest neighbor case by about 0.3 bits, 18 bits and, respectively, 14 bits. This shows that the cluster form is approximatively spherical for jpg, but not for median filtering and AWGN.

V. CONCLUSIONS

The robust hashing of ID photos proposed in this paper provides good results for non geometrical attacks. The method strength consists in including the registration points in the final hash. Unfortunately, for attacks like cropping, random line deletion, rotations or shifting, it represents an weakness. However, this may be compensated by using higher resolution ID photos or by allowing some freedom in image registration. Besides, the tests for stabilization by clustering suggest that a method adapted to non spherical clusters could give more robustness for our hashing.

ACKNOWLEDGMENT

This work was founded by UEFISCDI, Grant ID_1882/2008. The first author acknowledges the support of Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/6/1.5/S/19.

REFERENCES