Building Access Application Based on a Robust Biometric Watermarking Algorithm
Idrissi Nadia\textsuperscript{1}, Roukhe Ahmed\textsuperscript{1}, Lhoussaine Masmoudi\textsuperscript{1}

\textsuperscript{1}Department of physics, Faculty of Science, Moulay ismail University, B.P 11201 zitoune Meknes, Morocco
\textsuperscript{1}Department of physics, Faculty of Science, Mohammed V University, B.P 1014 4 avenue ibn battouta Rabat, Morocco

Abstract—We present an access control application that enables the authentication of the members of a building, this application uses a biometric watermarking algorithm based on a new robust method that uses various techniques such as, Eigen face, QR code, contourlet transform.

Several attacks have been applied to the watermarking algorithm, and they have proven its robustness. The tests performed on the graphical interface, showed the smooth running of the implementation of access control.

Keywords—access control, Eigen face, QR code, contourlet transform.

I. INTRODUCTION
The biometric watermarking is an integration of biometrics and the watermarking technology, to enhance the credibility of conventional watermarking methods. The combination of watermarking and the biometric features, helps to have a secure and confidential algorithm, since the biometric features are unique to each individual [1]. A biometric feature can be, face, iris, signature, the geometry of the fingers, hand geometry or voice. [2]

In this paper, we propose an access control application, which use a new biometric watermarking scheme, the algorithm apply several techniques such viola algorithm [6], PCA [7], QR code [8], wavelet transform, the contourlet transform, the different steps of the algorithm will be detailed in this work.

This application is intended to control the access to a building like a Laboratory, by using the biometric watermarking. The algorithm comprised three steps:

Step 1: data collection: we first detect faces by viola algorithm, then we extract the biometric features [10](biometric signature) by eigenfaces method based on PCA[11].

Step 2: Biometric watermarking: applying our approach [9] to insert in each detected face (step 1) its own biometric signature. In the end of this step we got a watermarked faces database.

Step 3: Decision-making: consists of two verification steps to strengthen the security of the access system:

• Checking if the presented image is watermarked or not.
• Comparing the signature detected during the first verification step with the data signatures of step1.

II. ACCESS CONTROLE APPLICATION
1. data collection
Firstly, we extract the faces from a group image, for this we used the ‘Vioala and Jone' algorithm [6].

![Fig. 1: faces detection](image)

Secondly, we apply the 'Eigen faces' method based on PCA on each face of the database B, to extract the biometric features.

1.1 Eigen faces
Face recognition method Eigen faces[10], employs the technique of principal component analysis. In the language of the theory of information, we want to extract relevant information from a face, encode it, then compare it to a models database encoded similarly.

www.ijaers.com
We choose the weight vector corresponding to the owner of the original image Bi, then we convert this vector into a QR code (cb), which will later be inserted into the image Bi. The insertion of the signature (QR code) is by applying our watermarking approaches [9].

Calculating the covariance matrix:
\[ C = \frac{1}{N} \sum_{i=1}^{N} \phi_i \phi_i^T = AA_i^T \] 

OR

\[ A = [\phi_1, \phi_2, \phi_3, \ldots, \phi_N] \]

\[ A = k^2 \times N. \]

3. implementation
After inserting the biometric signatures in the faces of the B database we used several test faces to verify the smooth functioning of our application.

The verification steps are described in this scheme.

Fig. 3: watermarking approach based on
III. EXPERIMENTAL RESULT

We divided the experimental results in two parts: the first is devoted to the analysis of the watermarking algorithm robustness against different types of attacks. The second is devoted to test the functioning of the access control application.

1. results of imperceptibility and robustness

Fig. 2: Diagram descriptive of the access control application

Table. 1: Results of imperceptibility
We note that the visual quality of the extracted image is good, we did not detect any damage at the extracted image or at the signature (QR code).

The table above describes the NC result after applying several attacks:

<table>
<thead>
<tr>
<th>Attaques /NC</th>
<th>Visage1</th>
<th>Visage2</th>
<th>Visage3</th>
<th>Visage4</th>
<th>Visage5</th>
<th>Visage6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salt and pepper noise (0.01 density)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Rotation (200)</td>
<td>1</td>
<td>0.995</td>
<td>0.996</td>
<td>1</td>
<td>0.995</td>
<td>0.995</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>0.998</td>
<td>1</td>
<td>0.999</td>
<td>0.998</td>
<td>1</td>
<td>0.999</td>
</tr>
<tr>
<td>Median filtering (3x3 kernel)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Resizing</td>
<td>0.991</td>
<td>0.992</td>
<td>0.990</td>
<td>0.993</td>
<td>0.990</td>
<td></td>
</tr>
<tr>
<td>Contrast adjustment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>JPEG QF=70</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table. 2: the result of the normalized correlation after attacks application.

The NC results show that our watermarking algorithm is robust to several types of attacks, and we note that after the application of all types of attack, we have could extract the QR code, and read the biometric signature. the robustness results prove the reliability of our watermarking algorithm, this allows us to move to the implementation of the access control application.

2. implementation of access control application

We used a GUI (Matlab guide) to facilitate the representation of our application.

The three faces used for the test:

unknown                  Laboratory members
algorithm, and the simulations show that our proposed approach is very feasible for a real application.

REFERENCES


As we have already mentioned, we used three test images to study the reliability of our application. Figure 3 shows that the three tests were done successfully.

IV. CONCLUSION

In this work we develop an application that controls the access to a building, the principle is to use the Eigen values as a biometric signature, and combined with the mechanism of QR Code to watermark a database of faces, that correspond to the members of the building. The biometric watermarking plays a vital role in the functioning of our application, it handles the authentication of the building members and decides to access or not. The results that we have presented in this work demonstrate the robustness of our watermarking

Fig. 3: Tests for the three faces