FACE SPOOFING ATTACK DETECTION BASED ON THE BEHAVIOR OF NOISES

Hoai Phuong Nguyen[⋆], **Florent Retraint**[†]
Frédéric Morain-Nicolier[⋆], **Agnès Delahais**[⋆]

[⋆] CREsTIC, Université de Reims Champagnes-Ardenne
[†] LM2S, ICD, Université de Technologie de Troyes

INTRODUTION

Authentication by facial recognition is actually one of the solutions to reinforce the security level of information systems. However, face recognition systems are proven to be vulnerable to spoofing attack. In fact, an attacker can bypass the authentification process easily by presenting in front of the camera a copy version of a legitimate user's face.

To make your face as your password, it is of vital importance to identify and reject the falsified faces photos. This work gives you a novel solution which exploits the inherent features of noises in digital images to detect falsified authentication.

NOISE LOCAL VARIANCE - NLV MODEL

NLV is the local variance of noise which is calculated within each 8x8 block of image.

Distribution of NLV values of a given image could be approximated by a Gamma distribution.

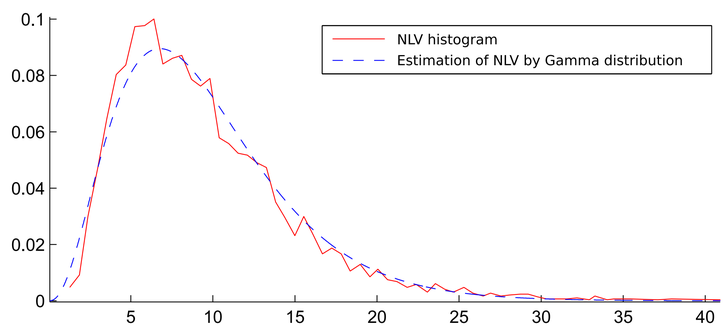

Figure 1: Distribution of NLV of an example image - the red continue curve is the histogram of NLV, the blue dashed curve is an estimation of the red one utilizing a Gamma distribution.

NLV FACE SPOOFING DETECTION FEATURES

Noise estimated from image is the sum of:

- **Acquisition noise** comes from various sources during the acquisition process: lighting conditions, imperfect instruments, photons conversion, compression and transmission loss,...
- **Textural noise** is caused by micro-textural information presenting on the surface of objects captured in the image.

By keeping unchanged some acquisition conditions (type of device, camera settings), acquisition noise can be hopefully maintained statistically stable between images. In these conditions, textural noise will play an important role which makes estimated noise statistically different between images of real face and fake face. In fact, textural information presenting in the surface of images of real face and fake face does not distribute as a same way.

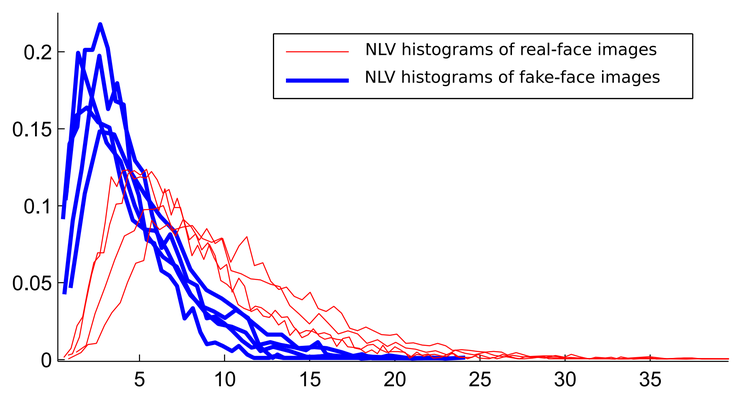

Figure 2: Difference in distribution of NLV histograms of different sets of images.

For a given family, there is a linear relation between the parameters of Gamma distribution fitting NLV histogram. The behavior of this linear relation is different between families of images.

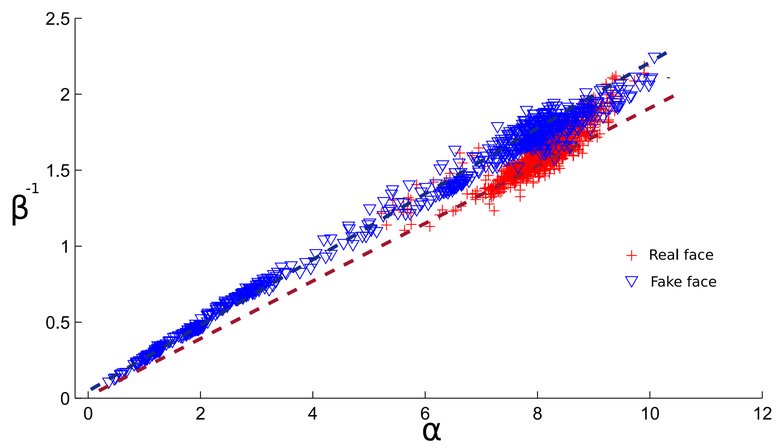

Figure 3: Scatter plot of the couples (α, β^{-1}); red cross correspond to real-face images, blue triangles correspond to fake face images

NLV Face Spoofing Detection Features:

- (α, β), the parameters of the Gamma distribution that fits the NLV histogram.
- Linear relation between α and β^{-1}

DETECTION SCHEME

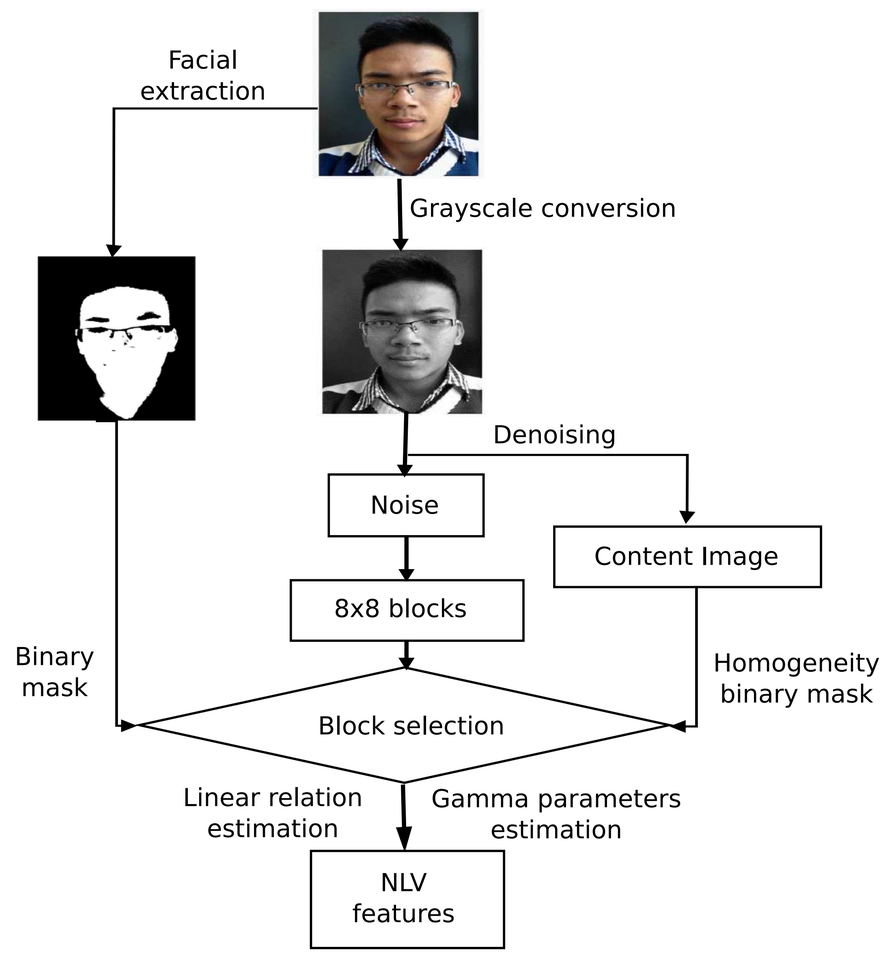

Figure 4: NLV Features Extraction Scheme

NUMERICAL RESULTS

Classification method: SVM

Database Characteristics:

Model	Real face images	Fake face images
iPhone5S	673	644
Samsung G.Alpha	722	911

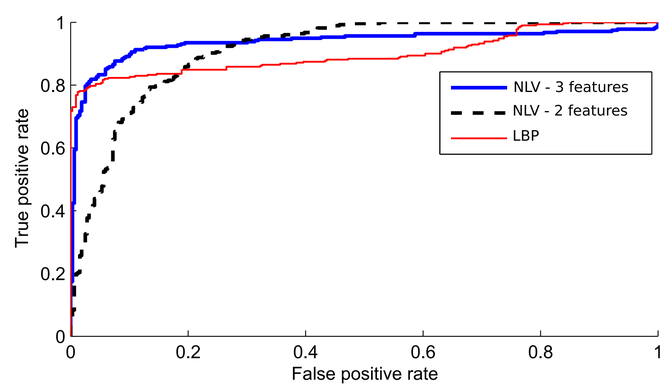

Figure 5: Perfomance (ROC cuvres) of the prososed method and the LBP method in discriminating real face images from fake ones. Studied images are taken by an iPhone 5S.

CONCLUSION

- The perfomance of the proposed method is promising for the two databases studied.
- Prior knowledge and some control of the acquisition system is required to obtain a good performance of detection. This requirement limits the field of application of the proposed method.
- The method could be improved by using a Statistical Hypothesis Test.

ACKNOWLEDGEMENTS

This work is financially supported by the group SURYS - Hologame Industries