False Negative issue in a face recognition authentication system

**Face recognition authentication system**

This Face detection authentication system is developed using python language with the support of opencv. Opencv’s built in LBPcascade classifier and LBPHFaceRecognizer is used in the system.

**How system works**

Initially when someone is going to register, camera feed is open in order to register the face. When registering 12 photographs of user is taken. In each of those photos face is separately detected using LBPcascade classifier. Those detected face information is stored as a numpy array with their corresponding coordinates.

Then LBPHFaceRecognizer is initialized and based on registration face information recognizer is trained.

Again, when user is going to log-in, video feed is open, and snapshot is taken. Then again face is detected in that snapshot and compared with trained model.

When system working properly system recognize the user and grant the access.

**Fault Negative Effect to the system**

Basically, this is happening cause to a security attack to the system. In False Negative Effect system should functioning correctly but authentication is not satisfied as expected.

In the system when someone register his face detected photographs are stored in a folder. When he is log in to the system, the face of user is compared with the detected faces of registration photographs.

But a third party can access registered-data folder and populate it with some fake data.

When such a situation happens even system is functioning 100% accurate original use cannot authenticate in to the system.

**Reasons for False Negativity**

Registration-data is not encrypted or protected. A third party can edit them easily.

Poor protection for registered data folder.

**Solution for False Negativity**

Protect Registration data as only privileged parties can edit the content.