Collaborative Algorithm for Reducing False Acceptance Error Rate of Face Recognition Based Admission Control System

Sagi Ben Moshe
Computer Science Department
Technion — Israel Institute of Technology, Israel
sagib@cs.technion.ac.il

Abstract

In this paper we discuss the problem of collaborative monitoring of unauthorized persons, trying to deceive a face recognition based admission control system. We propose an efficient collaborative scheme, based on the *TPP* algorithm proposed in [2], that relies on probabilistic local information flooding. Combining their collective knowledge, the various units of the system can identify malicious attackers trying to deceive the system and gain an unauthorized access. We analytically show that the False Acceptance Rate of the system is significantly reduced, using only $O(\ln n)$ messages sent by each unit (n being the number of cameras). This process is also shown to converge in $O(\ln n)$ time.

1 Introduction

Biometrics is the verification of an identity by the use of physiological or behavioral traits. The most prominent biometric technologies are fingerprint scanning, hand geometry, iris recognition, facial recognition, voice authentication, and dynamic signature verification. All biometric technology enablement necessitates four steps: sample capture, feature extraction, template comparison, and matching. This defines the biometrics process flow. One of the main usages for biometric systems is authentication — the act of confirming that an individual is who he or she claims to be. Accurate identification necessitates high-performance authentication. By enabling secure and convenient association of identity with authorized actions and credentials, accurate authentication enables confirmation of who an individual claims to be before access or transaction acceptance is granted.

Biometrics is used in a variety of industry segments, such as automotive, aerospace and defense, financial services, homeland security and law enforcement, medical devices, airports, education and more. The main segments of biometrics are fingerprint recognition, voice recognition, eye recognition, iris recognition, and facial recognition — being the fastest growing market segment, due to the advantages of new 3D technologies. Facial recognition systems analyze images of human faces for the purpose of identification. A facial recognition system identifies a person by comparing a newly captured image to a database of stored images. When the system is linked to a video surveillance system, an algorithm program is used to search for faces. Facial scan technology works well with commercial off-the-shelf (COTS) PC video capture cameras, and generally requires 320×240 resolution and at least three to five frames per second. Higher frame per second rates directly translate into higher performance. Facial recognition systems use programs that take facial images and measure the unique characteristics (geometry) of the face and create a template file. Using these templates, the software then compares the image with a stored image and produces a score that measures how similar the images are to each other. Typical sources of images in facial recognition include video camera signals and pre-existing photos, such as those in driver's license databases. Once the images are extracted, a template is created. The template is a compressed amalgamation of images and is usually less than $1/100^{th}$ the size of the original. The leading approaches in face recognition today are *Local Feature Analysis* (LFA) [7], *Laplacian-Faces* [5] and *Eigen-Face* [8].

Facial biometrics gets complex when lighting and angles change. Hence, face recognition performance suffers at longer distances. For example, conventional 3D face recognition cannot be used at distances beyond 2 meters without help of specialized surveillance cameras. People do not stop for cameras nor do they often look directly into the camera. Non-cooperative behavior creates angle and lighting variability that decreases accuracy. Two-dimension cameras have accuracy issues when a subject is in motion and as light varies. 3D biometrics can resolve this through multiple solutions, including infrared. However, 3D cameras are rather expensive, and

suffer from various problems typical for immature technologies.

As a result, most of currently available face recognition systems are subject to a relatively high levels of *False Accept Rate* and *False Reject Rate* which either compromise the reliability of the systems, or makes their use uncomfortable due to high level of False Rejection. Note that most systems can be calibrated such that there is a trade off between two error rates. Therefore, improving one of these features of the algorithm is expected to improve the overall usefulness of the system.

In this paper we propose a novel approach to reducing the False Acceptance error rate, and therefore significantly improving the usability of such systems. This is done using a collaborative algorithm, aiming for reducing the effect of malicious attacks on the system. The proposed method relies on the fact that although at certain times, certain cameras may mistakenly grant access to an unauthorized person, collaboratively processing these events may reduce the number of such cases dramatically. In order to do so, we use a collaborative algorithm for monitoring malicious applications in mobile phones, first proposed in [2]. Originally, this algorithm was designed to analytically guarantee that a dynamic mobile network would become immune to a stream of attacks by malicious applications. Adapted to the domain of collaborative face recognition, we show that this algorithm can also provide the ability to reduce the combined error rates of a system of face recognition cameras for admission control.

This paper is a position paper, presenting the problem and a proposed solution. Extensive simulation experiments will be carried out in the future, and reported in a full version of this paper. The rest of the paper is organized as follows : Section 2 presents the collaborative face recognition problem, while Section 3 presents our proposed solution. Theorem 1 shows an upper bound on the convergence time as well as the overall network overhead of the algorithm. Theorem 2 presents a lower bound over the improvement factor that is guaranteed by using the proposed algorithm, while Corollary 1 shows that this factor is monotonically increasing with the size of the network, n. Section 4 concludes the paper and discusses future work.

2 Face Recognition — Threat Model

Given a face recognition system, comprising n cameras, each having a *False Accept Rate* of λ_A and *False Reject Rate* of λ_R we are interested in implementing a coordination layer, on top of the existing system, that would guarantee a decreased error rates. We would also like this layer to have as small overhead as possible.

We assume that each camera can respond with 3 possible results, each time it is asked to grant access to a person : *Accept, Reject, Unsure*. When responding with *Unsure*, the system is assumed to treat this result as if it was *Accept*. Nonetheless, although for the person seeking access there are only two possible results (namely, *Accept, Reject*), the system can store the entries for which it had responded with an *Unsure* result.

Let $\hat{\alpha}$ denote a malicious person, disguised as an authorized person α, and occasionally recognized by the system as *Unsure*, with probability λ_M. We would like to minimize this probability. Notice that as $\hat{\alpha}$ actively tries to deceive the system, we can assume that its acceptance probability is greater than the average False Acceptance rate, namely : $\lambda_M \geq \lambda_A$.

We assume that $O(\ln n)$ reports that the same person was given access based on an *Unsure* result is enough in order to safely classify this person as a malicious attacker.

Let us assume that attacker $\hat{\alpha}$ encounters the system on average once every D days. We assume that the face recognition system is distributed (due to security considerations) but that units can pass messages on a random network overlay.

3 Collaborative Face Recognition Scheme

Definition 1. *Let λ'_A denote the new False Acceptance Rate of the system.*

Definition 2. *Let γ denote the improvement factor of the system. Namely, the ratio :*

$$\gamma \triangleq \frac{\lambda_A}{\lambda'_A}$$

In order to collaboratively monitor attack attempts on the system, we shall utilize the *TPP* collaborative monitoring algorithm, first presented in [2]. This algorithm was first developed in order to implement a collaborative monitoring scheme for mobile devices against malicious applications. The algorithm assumes that an agent is activated in any mobile device that chose to participate in this service. This agent periodically monitors one or more mobile applications, derives conclusions concerning their maliciousness, and reports its conclusions to a small number of other mobile devices. Each mobile device that receives a message (conclusion) propagates it to one additional mobile device. Each message has a predefined TTL. Upon receiving enough alerting messages (namely, more than a *decision threshold* ρ), a unit can classify an application as malicious. In this work we shall use the *TPP* algorithm for collaboratively monitor attacks against a distributed face recognition system. Every time a person seeking access would be recognized

with an *Unsure* result, the system would still grant this person access, but would react as though this was an application being identified as malicious. Namely, the unit would generate alerts messages and propagate them throughout the network. When a receiving unit had received more than ρ messages, it would stop granting access to this person, when it is recognized as *Unsure*.

Every D days, some of the n units of the system is approached by $\hat{\alpha}$ and in probability λ_M is accepted, with an *Unsure* result. In this case, the unit with which $\hat{\alpha}$ is currently engaged would generate an alert message, according to the *TPP* algorithm. This message would be propagated throughout the network of face recognition units, and would guarantee that after several encounters of some of the system's units with $\hat{\alpha}$, the vast majority of the units would be aware that the acceptance of $\hat{\alpha}$ is frequently done on the basis of its identification as *Unsure*. In this case, after a certain number of alerts is received, this person would be classified as malicious, and would no longer be granted admission access.

In order to verify that the system meets the requirements of the *TPP* algorithm, we would select its parameters as follows. The *TPP* algorithm guarantees that a large enough portion of the network is vaccinated against a given malicious threat. This portion equals $(1 - p_{MAX}) \cdot n$, where p_{MAX} denotes the penetration threshold of the system. Note that when the system is initialized person $\hat{\alpha}$ have admission access in probability of λ_M. Note also that relying on the properties of the *TPP* algorithm, once the algorithm converges the new acceptance probability of $\hat{\alpha}$ equals :

$$p_{MAX} \cdot \lambda_M \geq \lambda'_A$$

Therefore, we can calculate the correlation between the maximal penetration threshold p_{MAX} and the system's improvement factor, as shown in the next Lemma.

Lemma 1. *The improvement factor of the system can be lower bounded as follows :*

$$\gamma \geq \frac{\lambda_A}{p_{MAX} \cdot \lambda_M}$$

We shall now artificially set :

$$p_{MAX} = \frac{1}{\ln^2 n}$$

Theorem 1. *Using the* TPP *algorithm, an improvement factor γ of the False Acceptance Rate would be guaranteed after at most $O(\ln n)$ time, and using an average of $O(\ln n)$ messages sent by each unit.*

Proof. Observing Definition 1 of [2], we can see that we will meet the *Sparse Connectivity* requirements for all seeding factor p_N that satisfy :

$$p_N < \frac{T \cdot N}{n \cdot p_{MAX} \cdot (\rho + (\alpha + 1) \ln n)(1 - E_-)}$$

Which in our case means[1] :

$$p_N < \frac{\ln n}{n} \cdot D$$

Setting the seeding factor p_N as $\frac{\ln n}{n} \cdot D$ we can now proceed with the calculation of the value of TTL, as required by the *TPP* algorithm. Theorem 3 of [2] states that the TTL that alerting messages should be given must satisfy :

$$TTL = 4\sqrt{\frac{D \cdot \ln n}{n \cdot p_{MAX} \cdot p_N}} = 4 \ln n$$

Using Corollary 1 of [2], the rest is implied. □

The improvement factor of the system can now be calculated, as follows :

Theorem 2. *Using the* TPP *algorithm, the False Acceptance Rate of the system would be reduced by a factor γ, which can be lower bounded as :*

$$\gamma \geq \frac{\lambda_A}{\lambda_M} \cdot \ln^2 n$$

Proof. By assigning the value of p_{MAX} into Lemma 1. □

Corollary 1. *The improvement factor guaranteed by using the proposed method monotonically increases with the size of the network, n.*

4 Conclusions and Future Work

In this work we have presented a algorithm for collaborative face recognition, aimed for reducing False Accept and False Reject Error rates of any system of face recognition cameras. The algorithm relies on the *TPP* collaborative application monitoring algorithm, that was presented in [2]. Using the analytic properties of the *TPP* algorithm, we have shown that the error rates of any system comprising a multitude of face recognition cameras can be improved.

The improvement factor relies on the ratio of λ_A and λ_M, namely — what is the benefit of actually trying to deceive the system, compared to its "usual" False Acceptance Rate, and is given in Theorem 2. Corollary 1 shows that as can be expected due to the fact that the system is collaboratively using the collective experience

[1] Notice that this also guarantees connectivity of the network overlay, for all $D \geq 1$ [4].

of its units, the improvement factor grows monotonically with the size of the network.

The idea of collaboratively performing a face recognition mission was proposed in the past in the context of annotating photos for web and social networks applications [3, 6]. However, in this work we propose an automatic approach, analytically guaranteed to provide fast convergence, using low number of network overhead.

Another aspect of the proposed algorithm which is worth mentioning is the fact that the distributed face recognition units are assumed to be able to communicate short messages between one another. This can be implemented in several ways. Most trivially, adding our algorithm as an integral part of the face recognition system, this communication capability should be supported by the devices themselves. A second option would be the implementation of a complementary unit, to be added to existing off-the-shelve face recognition products, containing the proposed algorithm, as well as a communication device. A third option is to allow the devices to connect to existing service networks (such as the one discussed in [1]), thus saving on the design and implementation costs of a dedicated network facilitators.

In order to validate these results, an extensive experimental work is yet to be done, implementing this algorithm first in a simulated environment, and later — onboard real world systems. In addition, it would be interesting to examine the potential use of this approach for other biometric related problems, such as collaborative fingerprint recognition or collaborative voice recognition (not necessarily for security applications).

References

[1] Nadav Aharony, David P. Reed, and Andrew Lippman. Social area networks: Data networking of the people, by the people, for the people. In *CSE '09: Proceedings of the 2009 International Conference on Computational Science and Engineering*, pages 1148–1155, Washington, DC, USA, 2009. IEEE Computer Society.

[2] Yaniv Altshuler, Shlomi Dolev, Yuval Elovici, and Nadav Aharony. Ttled random walks for collaborative monitoring. In *NetSciCom 2010 (Second International Workshop on Network Science for Communication Networks)*, San Diego, CA, USA, 3 2010.

[3] Jae Young Choi, Wesley De Neve, Yong Man Ro, and Konstantinos N. Plataniotis. Face annotation for personal photos using collaborative face recognition in online social networks. In *DSP'09: Proceedings of the 16th international conference on Digital Signal Processing*, pages 240–247, Piscataway, NJ, USA, 2009. IEEE Press.

[4] P. Erdos and A. Renyi. On the evolution of random graphs. *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, 5:17–61, 1960.

[5] Xiaofei He, Shuicheng Yan, Yuxiao Hu, Partha Niyogi, and Hong-Jiang Zhang. Face recognition using laplacianfaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27:328–340, 2005.

[6] Stan Z. Li, RuFeng Chu, Meng Ao, Lun Zhang, and Ran He. *Advances in Biometrics*, volume 3832 of *Lecture Notes in Computer Science*, chapter Highly Accurate and Fast Face Recognition Using Near Infrared Images, pages 151–158. Springer Berlin / Heidelberg, 2005.

[7] S.P. Penio and J.A. Joseph. Local feature analysis: a general statistical theory for object representation. *Network: Computation in Neural Systems*, 7:477–500, 1996.

[8] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, pages 72–86, 1991.