

# On Matching Digital Face Images Against Scanned Passport Photos

Thirimachos Bourlai

Arun Ross

Anil Jain

**Abstract**—In this paper the problem of matching high-resolution digital face images against low-resolution passport photos scanned from the original document is studied. The challenges involved in such a problem are different from those encountered by classical face recognition systems described in the literature. The purpose of this paper is to illustrate the complexity of the passport face matching problem and to provide a preliminary solution to it. The contributions of this work are two-fold. First, a database of 25 subjects is assembled and used to illustrate the challenges associated with passport facial matching. Second, a pre-processing scheme is proposed in order to denoise and eliminate watermark traces that may be present in scanned passport photos. The application of such a pre-processing scheme is observed to improve the performance of face matching. To the best of our knowledge, this is the first time that this problem is being investigated in the open literature in the context of international passports exhibiting a variety of facial image qualities and security marks.

## I. INTRODUCTION

### A. Motivations

Significant progress has been made in the field of face recognition over the past decade as is borne out by the 2006 Face Recognition Vendor Test (FRVT) organized by NIST. For example, at a False Accept Rate (FAR) of 0.1%, the False Reject Rate (FRR) of the best performing face recognition system has improved from 79% in 1993 to 1% in 2006. However, the problem of matching facial images obtained under disparate ambient conditions using different imaging devices remains to be a challenging problem. Thus, unconstrained face recognition is an open research issue and has received considerably less attention in the literature [1].

This work concerns itself with an automated face recognition scenario that has been viewed as a challenging problem by several government agencies - that of comparing scanned photographs of the face against their high-resolution counterparts. Such a scenario is borne out in several applications including the need to compare face photos scanned from legacy passports against those obtained under controlled conditions. Other examples include matching face images present in driver's licenses, refugee documents, visas, etc., against digital photographs of live faces. As a case study, the specific problem of matching face images digitally scanned from passports against high-resolution digital face images is

T. Bourlai and A. Ross are with the Lane Department of Computer Science and Electrical Engineering at West Virginia University, Morgantown, West Virginia, U.S.A. Th.Bourlai@mail.wvu.edu, Arun.Ross@mail.wvu.edu

A. Jain is with the Departments of Computer Science & Engineering, and Electrical & Computer Engineering at Michigan State University, East Lansing, Michigan, U.S.A. jain@cse.msu.edu



Fig. 1. The mug-shots taken from passports issued by different countries: (a) Greece (issued 2006), (b) China (issued 2008), (c) US (issued 2008), and (d) Egypt (issued 2005).

explored. In this paper, this is referred to as *passport facial matching*.

Passport facial matching is a difficult problem involving factors that are quite different from that encountered by traditional face matching systems. These challenges can be grouped under three categories: person-related, document-related, and scanning device-related. Person-related factors include variations in hairstyle, expression, and pose of the individual. The photograph in the document is typically captured much earlier than its high-resolution counterpart, ranging from a few days to several years, thereby introducing an 'aging' factor as well. Document-related factors can significantly perturb the biometric content of the facial image; for example, security watermarks embedded on passport photos can distort the facial image thereby undermining its individuality. Other issues include variations in image quality, tonality across the face, and color cast of the photographs. Device-related issues are due to the foibles of the scanner used to extract face images from passports. By using a camera or scanner to 'scan' the passport photo, additional sources of noise may be introduced that can dete-



Fig. 2. A brief history of U.S. passport photographs. All are real passports apart from the 1935 passport replica. The images are available in the public domain [2].

riorate matching performance. These include limited device resolution, artifacts due to lighting, the smaller size of the document photo, the type of image file format/compression used, and operator variability. A few of the aforementioned problems are illustrated in Figure 1.

### B. Goals and Contributions

To the best of our knowledge, this paper represents the first attempt in the literature to investigate the problem of matching facial images scanned from international passports (issued in the last 3-4 years) that have been ‘contaminated’ with the latest security watermarks. The purpose of this work is to introduce the problem of passport facial matching and present the complexity associated with it. The contribution includes (a) an experiment that is designed to quantitatively illustrate the difficulty of the problem, and (b)

a pre-processing method to ‘restore’ the scanned passport photographs prior to comparing them against other face images.

In practice, the face image of a person can be gleaned from a passport document by capturing a digital image of the photograph page via a digital camera or a scanner. Then these photos can be compared against live face photos of the same person acquired using a high resolution digital camera. To facilitate this study, a database containing passport photos and face images of live subjects was assembled. Experiments were conducted using both a commercial as well as other standard face recognition algorithms.

### C. Paper Organization

The remainder of this paper is organized as follows. Section II presents the context to the problem, briefly reviews re-

lated work in the literature and highlights the key issues that are addressed in this work. Section III describes the proposed technique in detail. The empirical evaluation methodology, data sets used and the results of the experiments are reported and discussed in Section IV. The paper concludes with a summary and an outline of promising directions for future research in Section V.

## II. BACKGROUND

### A. History

The history of passport goes back to the time of the Persian Empire in about 450 BC when Nehemiah (an official serving King Artaxerxes I of Persia), received a letter from the king to the “governors beyond the river” so that he could travel to Judea safely (Nehemiah 2:7-9). Then in 1791, the adventurer Philip Nolan obtained a passport from the governor of Louisiana for his first documented trip into Texas [3]. At that time passports included only a description of the passport holder and the purpose of the trip.

Attachment of photographs to passports began in the late nineteenth century and became very popular in the late twentieth century when photography became widespread. However, every country tried to develop its own standard for passports resulting in a disparity of these documents across the world. In 1963 the United Nations held a travel related conference but passport guidelines did not emerge from it. Passport standardization came about in 1980, under the auspices of the ICAO - the International Civil Aviation Organization.

Passport documents have changed frequently, especially within the last decade, to meet the security needs of contemporary society. A visual representation of the brief history of US passports is presented in Figure 2 [2]. Notice that after 1985, there has been an increase in the security marks used to guard against forgery. However, in the more recent passports (2009) the image quality is severely impacted and the tonality across the face is diminished. A security watermark is observed to run across the forehead of the bearer’s photograph, and there is a strong magenta cast on the photograph that can deteriorate the ability to identify the bearer.

Within the last decade *biometric passports* or *e-passports* have appeared internationally. Critical information pertaining to the subject is printed on the data page of the passport as well as stored in a microprocessor chip. Based on directives provided by the ICAO, a subset of the face, fingerprint and iris identifiers may be embedded in these passports. However, not all passports are biometric and in the event that the digital biometric information stored in a biometric passport is damaged or rendered inaccessible, then the mug-shot of the bearer as it appears on the passport can be used. Thus, the problem addressed here is very relevant for border control situations today.

### B. Related Work

No work has been reported in the literature that addresses the problem of passport facial matching using *international*

passports. Staroviodov et al. [4], [5] presented an automated system for matching face images present in documents against camera images. The authors constrained their study to the previous generation of passports pertaining to a single country. Further, in the images considered in their work, the facial portion of the photograph was reasonably clear and not ‘contaminated’ by any security marks (see Figure 3). Thus, the system’s ability to automatically identify the face photograph was not severely compromised.



Fig. 3. Examples of face patterns obtained from older generation passports issued by the same country [4].

Passport technology has changed significantly since 1985 when the use of glue for affixing photographs was replaced with the use of lamination on the photo page. More recently, the entire page/photo is digitally generated. The result is a photograph where the face of the bearer may be contaminated with noise (as described in Section I). However, the *nature* of noise differs across passports of different countries. Thus, the watermarks present in European Union passports are quite different than that in a United States passport, an Asian or a Middle East one. Figure 1 clearly illustrates such a case. These examples further highlight the complexity of the problem.

## III. PROPOSED TECHNIQUE

### A. Hardware and Settings

The devices used in this research for scanning passport photos were a NIKON Coolpix P-80 digital camera <sup>1</sup> and

<sup>1</sup>www.nikonusa.com/Find-Your-Nikon/Product/Digital-Camera/26114/COOLPIX-P80.html

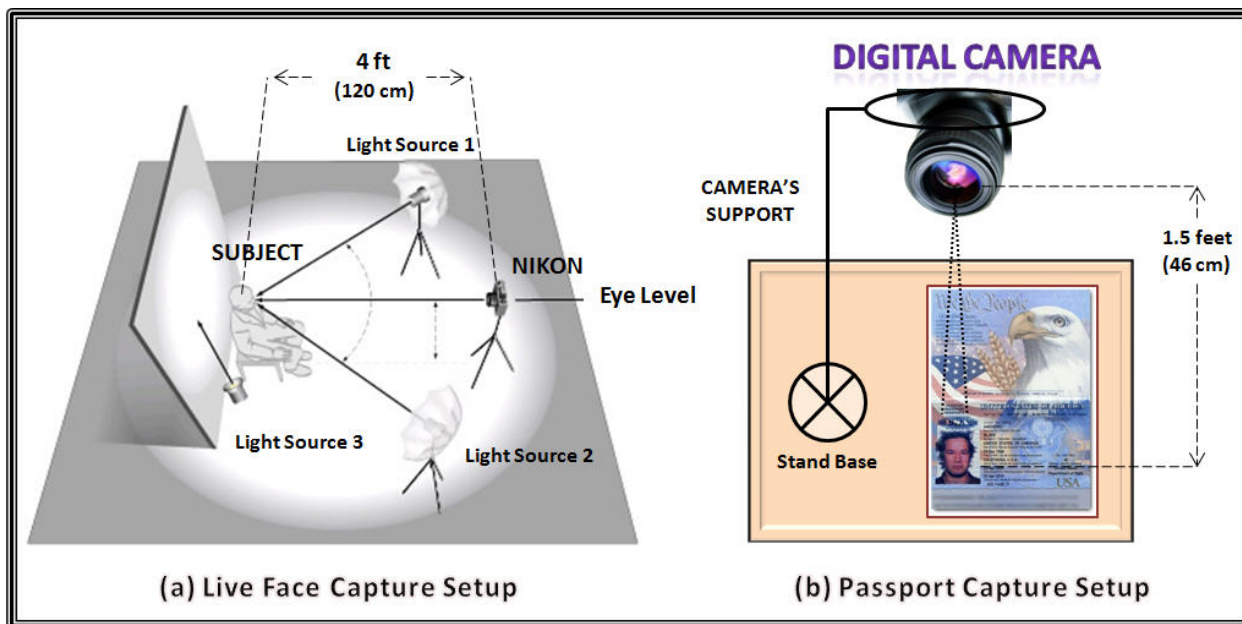


Fig. 4. Image capture setup: (a) The live subject-capture setup (taken from the US Department of US State Department, Bureau of Consular Affairs). More details have been added by the authors. (b) The passport-capture setup used for data collection.

a HP Office jet Pro L7780 Scanner <sup>2</sup>. The NIKON digital camera was also used to obtain a high-resolution face image of the live subject. The NIKON camera parameters in both these cases were set to the following: maximum resolution (10.1 Mega pixels - 3648 × 2736), Auto-Focus, Optical Vibration Reduction Image Stabilization, Portrait Mode, ISO AUTO, In-Camera Red-Eye Fix, and JPEG format. The HP scanner was set to acquire high quality color images with a maximum resolution of 5.8 Mega pixels - 2900 × 2000 - in the JPEG format.

**B. Face Capture Setup**

The live face capture and passport capture setups for data collection are shown in Figures 4 (a) and (b), respectively. Note that the live face capture setup is based on the US government guidelines to acquire the passport and visa photos of travelers <sup>3</sup>. This is illustrated in Figure 4 (a). In the case of the HP scanner, a typical document scanning process was followed to obtain the photograph on the passport page.

**C. Data Collection Process**

The above configurations were used to acquire data from 25 subjects, i.e., 4 from Europe, 11 from United States, 5 from India, 2 from Middle East, and 3 from China; the age distribution of these participants was as follows: 20-25 (9 subjects), 25-35 (10 subjects), and over 35 (6 subjects).

The subjects were briefed about the data collection process after which they signed a consent document. During the collection of high-resolution face images from live subjects, the subject was asked to sit ~4 feet away from the camera (see Figure 4 (a)). When photographing the passports, the camera

was placed about 1.5 feet vertically above the passport. The passport had a fixed position on the table so that the page with the face of the bearer was not bent (see Figure 4 (b)).

**D. Passport Database**

The data collection process resulted in the generation of the Passport Database (PassportDB) composed of three datasets, i.e., the NIKON Face Dataset (NFaceD) containing high-resolution face photographs from live subjects, the NIKON Passport Face Dataset (NPassFaceD) containing images of passport photos, and the HP Scanned Passport Face Dataset (HPassFaceD) containing face images scanned from the photo page of passports.



Fig. 5. Samples of a subject taken from the three datasets of PassportDB.

The NPassFaceD and HPassFaceD were assembled during the first session. In the case of NPassFaceD, three samples of the photo page of the passport were acquired for each subject. Multiple samples were acquired to compensate for the reflections on the laminated paper as well as the motion of the camera operator. In the case of HPassFaceD, one scan (per subject) was sufficient to capture a reasonable quality mug-shot from the passport. Figure 5 illustrates three

<sup>2</sup>www.shopping.hp.com/store/product/product\_detail/C8192A%2523ABA  
<sup>3</sup>http://travel.state.gov/passport/guide/setup/setup\_873.html

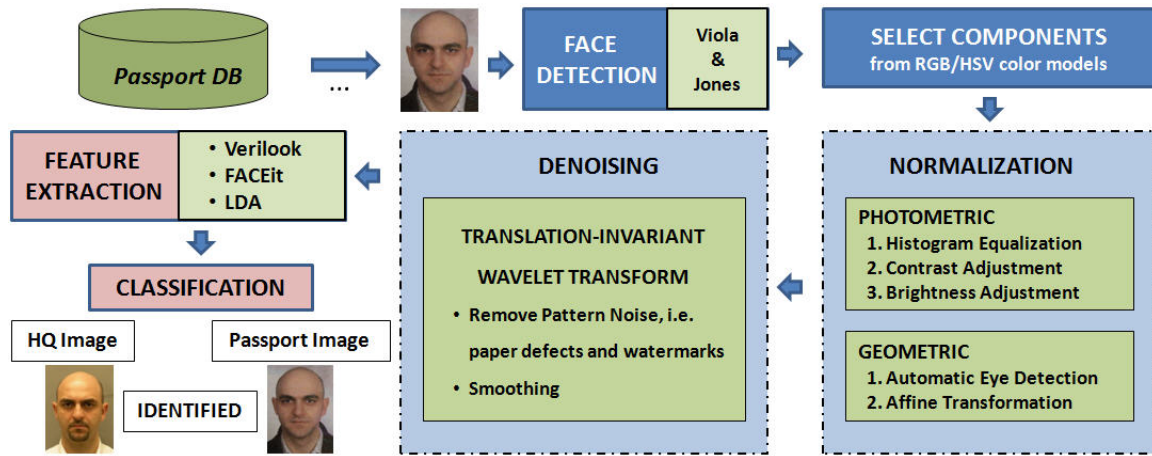


Fig. 6. Overview of the methodology used when passport mug-shots are used to test the system.

samples of a subject present in the three datasets of the PassportDB.

#### IV. EMPIRICAL EVALUATION

##### A. Face Recognition Systems

Though early approaches to face recognition were based on geometrical features (such as nose width and length, mouth position and chin shape), nearly all of the applicable approaches developed in recent years are based on a combination of global and local texture representations [6][7]. The most commonly used statistical representation for face recognition and verification is the Karhunen-Loeve (KL) expansion [8] which is also referred to as Principal Components Analysis (PCA) or the eigenfaces method [9][10]. While PCA has proved to be very effective for information compression, it does not guarantee the most efficient compression of discriminatory information. The *Linear Discriminant Analysis* (LDA) was suggested for face recognition by Belhumeur et al. [11] where the LDA representation was demonstrated to outperform the PCA representation. More recently, a variety of texture models and deformation models have been used for face recognition [12]. In this work LDA, which is an appearance-based method, is used in combination with the *k*-nearest neighbor algorithm (*k*-NN) [13], [14].

The techniques employed to perform the recognition experiments include:

- 1) Commercial software provided by Verilook [15].
- 2) Commercial software *FaceIt*<sup>®</sup> provided by L1 Systems<sup>4</sup>.
- 3) Linear Discriminant Analysis in combination with the *k*-Nearest Neighbor (*k*-NN) algorithm.

##### B. Experiments

Three different experiments were conducted. In *Experiment 1 (Exp 1)*, *Session 1* of the NFaceD dataset was used for *training* (175 images, i.e. 25 subjects with 7 images per subject), and *Session 2* was used for *testing* (175 images, i.e. 25 subjects with 7 images per subject). In both cases the

Viola & Jones algorithm was employed for face detection [16]. The focus of this paper is on *Experiment 2 (Exp 2)* and *Experiment 3 (Exp 3)* where the system is trained with all samples from both sessions of the NFaceD dataset (350 images, i.e. 25 subjects over 2 Sessions with 7 images per subject). Then system performance is tested with the passport mug-shots acquired by the NIKON digital camera (75 images, i.e. 25 subjects with 3 images per subject), and the HP scanner (25 images, i.e. 25 subjects with 1 image per subject). In *Exp 2*, 3 samples per subject of the NPassFaceD dataset were used for testing, and in *Exp 3* a single sample per subject of the HPassFaceD dataset was used for testing. *Exp 2* was also used to study the effects of face normalization and denoising (as described in Section IV-C) on system performance. A summary of the data used in the experiments performed is presented in Table I.

TABLE I  
SUMMARY OF THE DATA USED IN THE THREE MAIN EXPERIMENTS, AS WELL AS THE PRE-PROCESSING EXPERIMENT

EXPERIMENT	Train	Test
1	NFaceD(S1)	NFaceD(S2)
2	NFaceD(S1/S2)	NFacePassD
3	NFaceD(S1/S2)	HFacePassD
Pre-Processing	NFaceD(S1/S2)	NFacePassD

##### C. Methodology

The methodology proposed for passport facial matching is illustrated in *Figure 6*. The salient stages of the proposed method are described below:

- 1) *Face Detection*: The Viola & Jones face detection algorithm is used to localize the spatial extent of the face and determine its boundary. The algorithm was observed to perform reasonably well on the face images acquired in this work.
- 2) *Channel Selection*: Since the images are acquired in the RGB color domain, it is important that an appropriate color space transformation be determined for further processing. Empirically, it was determined that in the

<sup>4</sup>epic.org/privacy/surveillance/spotlight/1105/facefaqs.pdf

majority of passports the Green channel (from the RGB color space) and the Value channel (from the HSV color space) are less sensitive to the effects of watermarking and reflections from the lamination. These two channels were selected and then added resulting in a new single-channel image.

- 3) *Normalization*: In the next step, photometric and geometric normalization schemes are applied to the original images (Fig. 7(b)). The normalization scheme compensates for poor image contrast and slight perturbations in the frontal pose. *Geometric normalization* is composed of two main steps, viz., eye detection and affine transformation. Eye detection (Fig. 7(c)) is based on a template matching algorithm. Initially, the algorithm creates a "global eye" from all subjects, and then it detects, for each subject, both the eyes based on a cross correlation score between the global and the target eye.

Based on the eye coordinates obtained by eye detection, the canonical faces are constructed by applying affine transformation as shown in Fig. 7. Faces are first aligned by placing the coordinates of the eyes in the same row so that the slope between the right and left eye is zero degrees. Then the distance between the eyes is computed and the image is cropped based on a pre-defined spatial resolution, removing most of the background and hair. Eventually, all faces are warped to the same dimension of  $300 \times 300$  as shown in Fig. 7(d) from their original form as in Fig. 7(b).

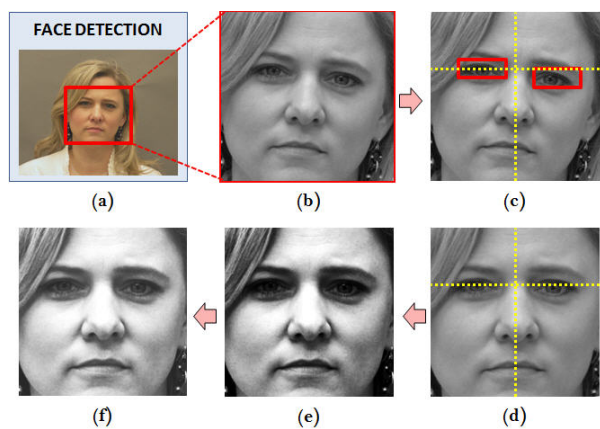


Fig. 7. Overview of the methodology used to perform face normalization. (a) Face detection; (b) Convert to gray scale; (c) Eye detection; (d) Geometric Normalization; (e) Histogram Equalization; (f) Contrast/Brightness Adjustment.

*Photometric normalization* is employed in order to achieve illumination correction. It is also composed of two main steps, viz., histogram equalization and contrast/brightness adjustment. Histogram equalization is a non-linear image enhancement method which transforms image brightness in such a way that it is particularly suited to human visual analysis. It is very useful in face verification systems since it improves the verification performance [17]. Finally, contrast and

brightness adjustment was employed. Both steps are illustrated in Figures 7(e,f).

- 4) *Denoising*: A denoising algorithm based on wavelets is applied to remove the additive noise present in the passport face images. The problem of image de-noising [18] can be summarized as follows. Let  $F(i, j)$  be the noise-free image and  $Y(i, j)$  be the image corrupted with independent Gaussian noise  $Z(i, j)$ :

$$Y(i, j) = F(i, j) + \sigma \cdot Z(i, j), \quad (1)$$

where  $Z(i, j)$  is assumed to have a normal distribution  $N(0,1)$ . The problem is to estimate the desired  $F(i, j)$  as accurately as possible according to some criteria. The application of a traditional (orthogonal) de-noising wavelet transform sometimes results in visual artifacts. Some of those are attributed, for example, to the Gibbs phenomena in the neighborhood of discontinuities. This is due to the lack of translation invariance of the wavelet basis. In order to suppress such artifacts, Coifman et al. proposed the *Translation-Invariant Wavelet Transform* (TI-WT). It is a denoising algorithm that averages out the translation dependence [19]. This algorithm is used to suppress the effects of noise. The steps of de-noising the passport facial images using the TI-WT are summarized below:

- a) Apply Discrete Wavelet Transform (DWT) to the noisy face image by using a Daubechies wavelet.
- b) Apply hard-thresholding to obtain the estimated wavelet coefficients (gives better results than soft-thresholding).
- c) Reconstruct the denoised face image from the estimated wavelet coefficients, by applying the Inverse Discrete Wavelet Transform (IDWT).

This algorithm was used to remove the pattern noise from the passport face images, i.e. any spatial pattern that does not change significantly from image to image. Major sources of pattern noise in a passport photo are paper defects and watermarks. Digital watermarks are used for integrity verification and are placed on the passport photo forming a dynamic pattern. Depending on the capture angle and the light sources in the environment, the watermarks can be pronounced. In addition, each country's passport has its own watermark and there is no generic way to properly remove them. It is necessary to minimize their visual effect on each passport facial photo for further processing. The proposed denoising algorithm removes most of the watermarks. However, the denoising level has to be carefully selected for each image. This level was manually adjusted in this work.

Figure 8 illustrates the effect of applying the denoising algorithm. Figure 8 (a) shows an example of a scanned passport face image, and Figure 8 (b) zooms into a specific Region Of Interest (ROI). In Figure 8 (c) the grayscale version of the ROI before applying the TI-WT can be seen. Finally, Figure 8 (d) illustrates that

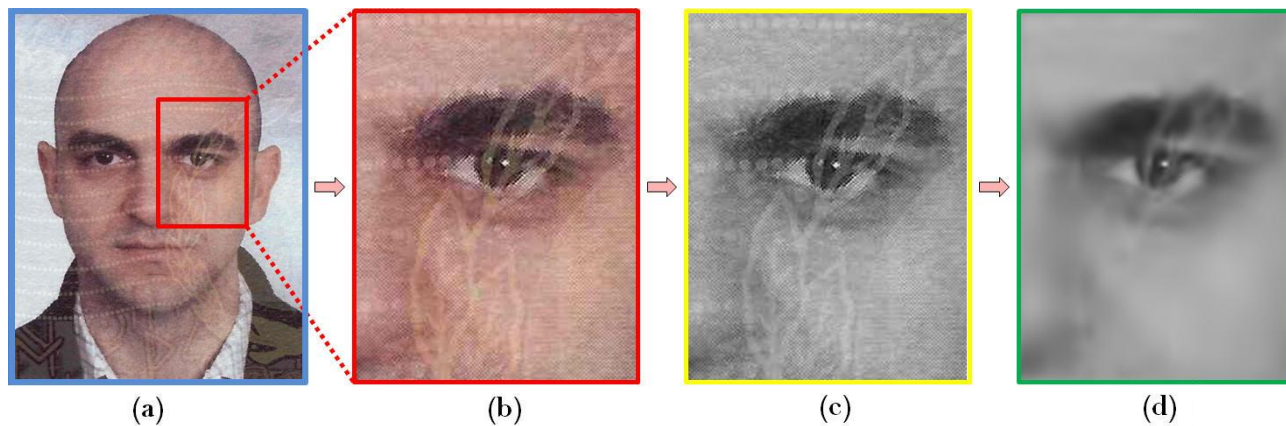


Fig. 8. Illustration of denoising: (a) A sample scanned passport face image taken from the HPassFaceD dataset; (b) selected ROI; (c) grayscale version of the ROI before denoising is applied; (d) ROI after denoising.

when the denoising algorithm is applied, most of the pattern noise is removed.

- 5) *Feature Extraction and Classification*: The methods described in Section IV-B are then used to perform matching and generate match scores.

#### D. Performance Evaluation

To evaluate the performance of the system, the Equal Error Rate (EER) criterion is employed (other measures such as d-prime or the FRR at a pre-defined FAR may be used). This is determined from the Receiver Operating Characteristic (ROC) Curve [20] computed on the test sets, i.e. the NPassFaceD and the HPassFaceD datasets. The lower the EER, the better is the system’s performance.

#### E. Results

1) *Effect of Pre-Processing*: The main effects of face normalization and denoising on system performance were studied in the case of *Exp 2*. The impact of each normalization step is presented in *Figure 9*. It can be seen that each step contributes to improvement in matching performance. By carefully selecting the right components from each of the RGB and HSV color models, respectively, and adding them up, face images with lower noise content are obtained. However, this step only provides a slight advantage in terms of performance. The face normalization step is more important (EER improves by more than 9%) compared to denoising (which brings down the error by another 5.8%). Finally, by removing some really bad passport face samples, further improvement in performance can be observed.

2) *Pre- vs. Post-Processing Effects*: In *Exp 1*, the system is trained with *Session 1* of the NFaceD dataset and tested with *Session 2*. In the remaining experiments, the system is trained with all available images of the NFaceD dataset, and tested with the NPassFaceD and HPassFaceD datasets, before and after applying the pre-processing schemes (i.e., denoising, normalization and watermark removal). Experimental results are presented in *Table II*, *Figure 10*, and *Figure 11*.

In the case of *Exp 1* involving high resolution face images, application of the FaceIt commercial software resulted in

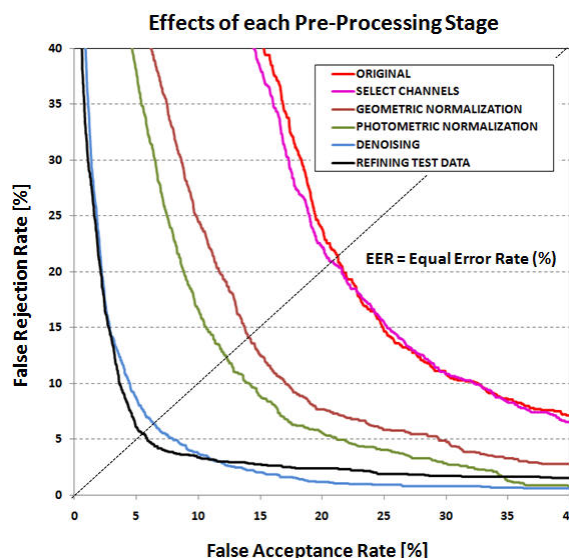


Fig. 9. The effects of face normalization and denoising on system performance. The experiments were conducted by using all available images of the NFaceD dataset for training and the images from the NPassFaceD for testing.

~0.6% EER whilst the Verilook software resulted in an EER greater than 1%. The LDA with k-NN classifier resulted in about 3.5% EER. Reduction in performance was observed when the system was tested with the highly degraded scanned passport photos. This represents a true border control scenario where the face recognition system may be trained on high quality face images but tested on poor quality ones. In both *Exp 2* and *Exp 3*, Verilook’s feature extraction process failed in several cases, and did not generate the scores necessary for further analysis. In the case of FaceIt, the software did generate the necessary scores but resulted in inferior matching performance.

It appears that the commercial software used in this work were not designed to extract features from such degraded images. This coupled with the fact that a very small test data was used in *Exp 3*, may have led to their inferior performance

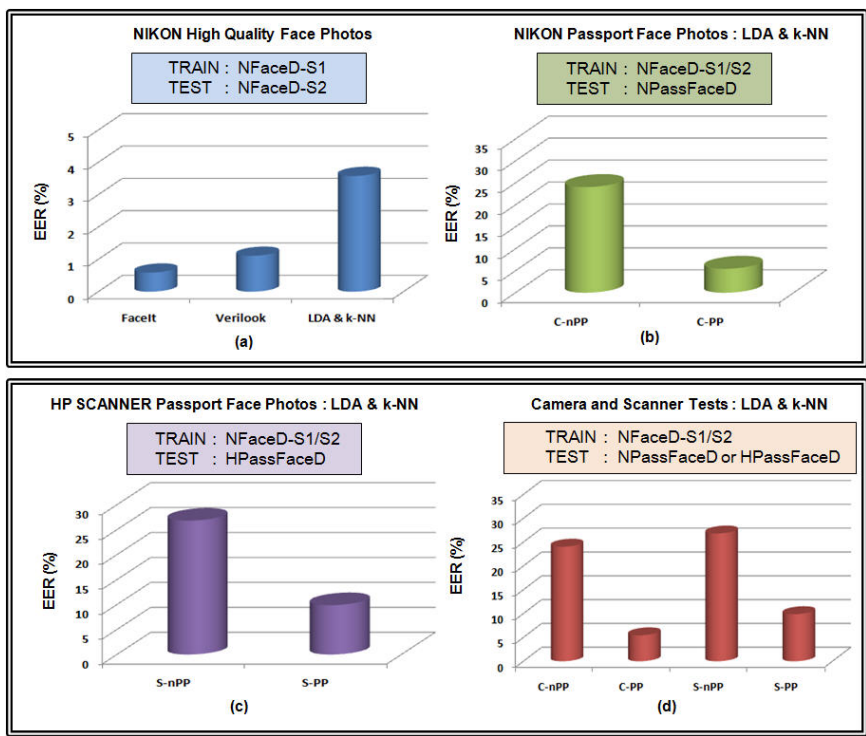


Fig. 10. (a) Performance of face recognition systems when training/testing with the high resolution digital face images. (b) Results when only the digital camera is used. The system is trained with the high-resolution face photos and tested with the digital camera *passport* face photos, before and after applying pre-processing. (c) Results when only the scanner is used. The system is trained with the high-resolution face photos and tested with the scanner *passport* face photos, before and after applying pre-processing. (d) Comparison among all testing scenarios when the LDA&k-NN system is used for matching. C = Camera; S = Scanner; nPP = no Pre-Processing; PP = Pre-Processing.

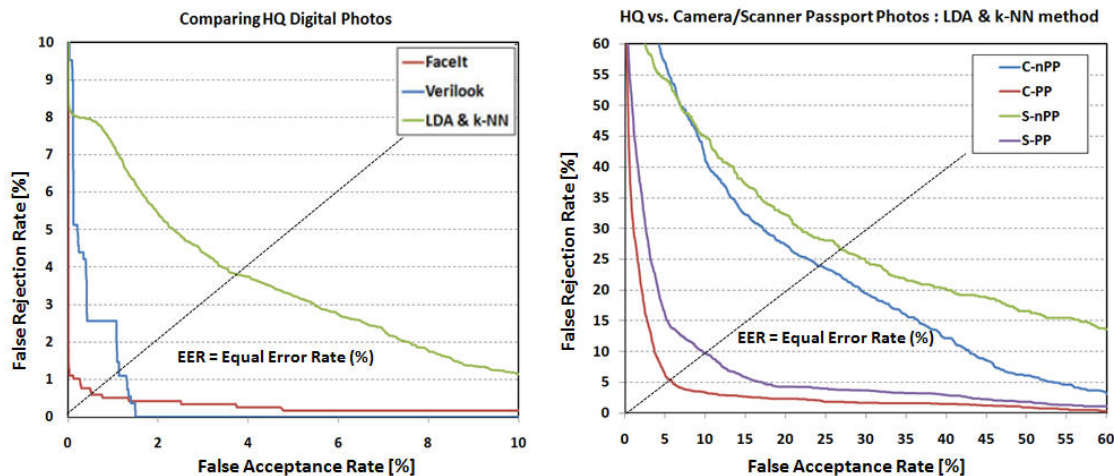


Fig. 11. The ROC curves of the results presented in Figure 10.

on this challenging dataset. The LDA with k-NN technique, however, was successful in all three experiments (i.e., the feature extraction and matching stages were successfully executed).

Experimental results show that when testing the system with passport photos, the recognition performance improves after denoising and photometric normalization are applied to images in both the training and test sets.

These results indicate that the problem of passport face matching is far from being solved. More studies are nec-

essary to further improve the recognition accuracy. Different modeling approaches need to be developed, and more experiments are necessary with some of the leading FRGC/FRVT/MBGC technologies.

## V. SUMMARY AND FUTURE DIRECTIONS

### A. Summary

This paper addresses the problem of matching digital face images against passport photos. The challenges involved in



TABLE II  
PERFORMANCE RESULTS IN TERMS OF EER OF ALL  
EXPERIMENTS. S1/S2=SESSION 1/2;  
PRE-PROC=PRE-PROCESSING.

Train	Test	Pre-Proc	Method	EER (%)
NFaceD(S1)	NFaceD(S2)	-	FaceIt	0.59
NFaceD(S1)	NFaceD(S2)	-	Verilook	1.11
NFaceD(S1)	NFaceD(S2)	-	LDA & k-NN	3.58
NFaceD(S1/S2)	NFacePassD	No	FaceIt	70.83
NFaceD(S1/S2)	NFacePassD	No	Verilook	-
NFaceD(S1/S2)	NFacePassD	No	LDA & k-NN	24.05
NFaceD(S1/S2)	NFacePassD	Yes	FaceIt	48.70
NFaceD(S1/S2)	NFacePassD	-	Verilook	-
NFaceD(S1/S2)	NFacePassD	Yes	LDA & k-NN	<b>5.49</b>
NFaceD(S1/S2)	HFacePassD	No	FaceIt	47.02
NFaceD(S1/S2)	HFacePassD	No	Verilook	-
NFaceD(S1/S2)	HFacePassD	No	LDA & k-NN	26.82
NFaceD(S1/S2)	HFacePassD	Yes	FaceIt	58.11
NFaceD(S1/S2)	HFacePassD	-	Verilook	-
NFaceD(S1/S2)	HFacePassD	Yes	LDA & k-NN	<b>9.89</b>

such a problem are due to factors associated with subjects, documents, and scanning devices.

There are several reasons why the matching accuracy between passport photos and the corresponding high resolution photos is low. Different passport photos exhibit different image quality and have various types of security marks embedded in them. Interestingly, even with passports from the same country, the watermarks were observed to be different. Another problem is the aging factor since the face image in the passport may be obtained at a significantly different time than its high resolution counterpart. In such cases, even a human operator may not be able to easily deduce the identity of the passport photo (e.g. subjects (2) and (8) in *Figure 12*).

A series of experiments were conducted to demonstrate that passport facial matching is a challenging problem that can be addressed to a moderate extent by adopting ad-hoc methodologies in spite of the aforementioned difficulties. Better results are achieved when testing using the photos acquired with the Nikon digital camera rather than with those acquired with the scanner. The application of the pre-processing scheme resulted in a performance boost when employing the LDA-based model.

It is interesting to note that while both the commercial software obtained less than 1.2% EER on the high-resolution digital photos from live subjects, they did not work well in both the passport facial matching scenarios. This suggests that passport images are not easy for automated face recognition; this was one of the reasons why the LDA and k-NN classifier was used in this work. The other was to standardize the process and show that the application of a pre-processing technique results in improved matching accuracy.

Experimental results showed that the LDA and k-NN classifier achieved a 5.49% EER when testing the system with the passport dataset acquired using the digital camera, and 9.89% EER when testing the system with the passport dataset acquired by the scanner. These results are reasonable compared with the 3.58% EER achieved when the system is trained/tested with the high resolution face images.

### B. Future Directions

It is possible that in the near future, there will be e-passports and/or other government documents that will incorporate a flexible combination of security features, which will make credential forgery and manipulation all but impossible. It is expected that a combination of features such as tactical laser engraving, color re-transfer printing, high resolution ultraviolet printing, multiple and/or changeable laser images, etc. will become common-place in future documents. However, until the time such a technology is adopted worldwide, there will be many instances where government agencies (e.g., border control officers) will benefit from techniques that can perform passport facial matching.

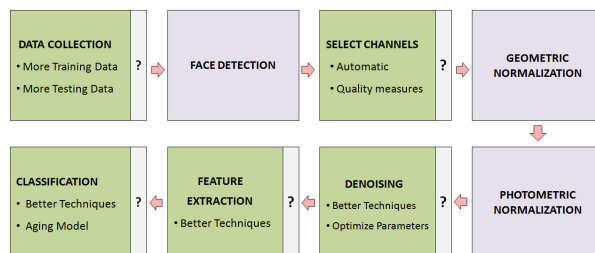


Fig. 13. Modules used in passport face matching. The question marks highlight the modules that need to be more effectively addressed in the future.

The problem of passport facial matching, as defined in this paper, needs to focus more on the pre-processing methodologies. The use of an aging face model would also improve the accuracy of the system [21]. More tests should be conducted where leading FRGC/FRVT/MBGC face recognition technologies are employed for comparison. An overview of the proposed approach and the modules that need to be improved in the future are presented in *Figure 13*.

### ACKNOWLEDGMENTS

This work was funded by the Center for Identification Technology Research (CITeR) at WVU. The authors are grateful to Arvind Jagannathan for assisting with the data collection process and to Raghavender Jillela for assisting with the experiments.

### REFERENCES

- [1] Shaohua Kevin Zhou, Rama Chellappa, and Wenyi Zhao. Unconstrained face recognition. *Springer Publishers*, pages 1–8, 2006.
- [2] B. Andrew. A brief history of US passport photographs. [blakeandrews.blogspot.com/2009/05/brief-history-of-us-passport.html](http://blakeandrews.blogspot.com/2009/05/brief-history-of-us-passport.html), May, 2009.
- [3] D. L. Thrapp. Encyclopedia of frontier biography. *University of Nebraska Press*, 2(G-O):1060–1061, 1991.
- [4] V. V. Starovoitov, D.I. Samal, and B. Sankur. Matching of faces in camera images and document photographs. *Int. Conf. on Acoustic, Speech, and Signal Processing*, IV:2349–2352, June 2000.
- [5] D. V. Briliuk V. V. Starovoitov, D. I. Samal. Three approaches for face recognition. *Int. Conf. on Pattern Recognition and Image Analysis*, pages 707–711, October, 2002.
- [6] R. Brunelli and T. Poggio. Face recognition: Features versus templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(10):183186, 1993.
- [7] W. Zhao, P.J. Phillips, R. Chellappa, and A. Rosenfeld. Face recognition: A literature survey. *ACM Computing Survey*, page 399458, 2003.

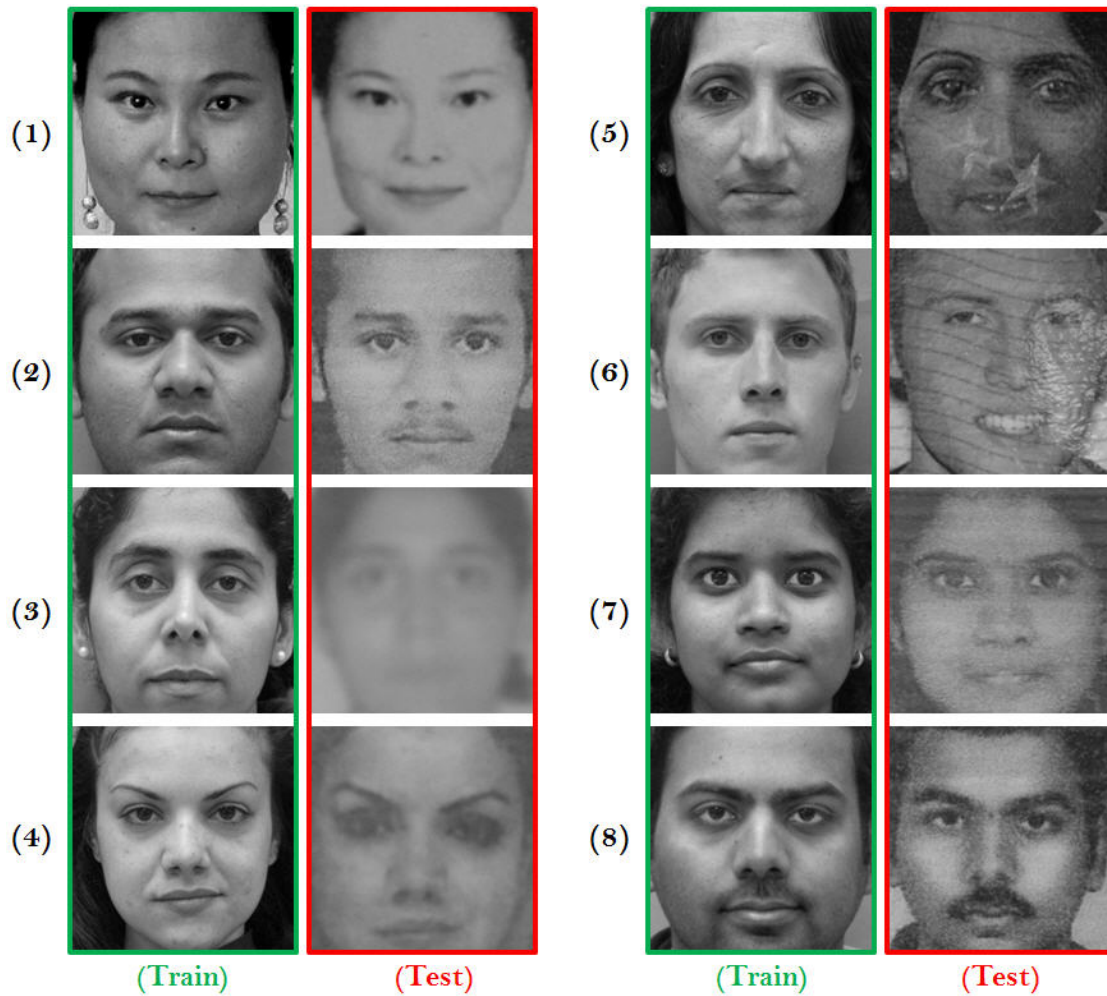


Fig. 12. Example training (taken from the NFaceD dataset) and test (taken from the NPassFaceD and HPassFaceD datasets) images that clearly illustrate the problem of passport facial matching.

[8] A. P. Devijver and J. Kittler. Pattern recognition: A statistical approach. *Prentice-Hall, Englewood Cliffs, N. J.*, 1982.

[9] L. Sirovich and M. Kirby. Application of the karhunen-loeve procedure for the characterization of human faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 12(1):103–108, 1990.

[10] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1):7186, 1991.

[11] J. Hespanha P.N. Belhumeur and D. J. Kriegman. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19:4558, 1996.

[12] S. Z. Li and A. K. Jain, editors. *Handbook of Face Recognition*. Springer, 2005.

[13] T. M. Cover and P. E. Hart. Nearest neighbor pattern classification. *IEEE Trans. Inform. Theory*, 13(1):2127, 1967.

[14] E. Fix and J. L. Hodges. Discriminatory analysis, nonparametric discrimination: Consistency properties. *Technical Report 4, USAF School of Aviation Medicine, Randolph Field, Texas*, 1951.

[15] Neurotechnology. Verilook 3.2 sdk for face recognition. <http://www.neurotechnology.com/face-biometrics.html>, 2009.

[16] Paul A. Viola and Michael J. Jones. Robust real-time face detection. *International Journal of Computer Vision*, 57(2):137–154, 2004.

[17] Y. P. Li, J. Kittler, and J. Matas. Analysis of the lda-based matching schemes for face verification. *British Machine Vision Conference*, 2000.

[18] S. Kother Mohideen, S. Arumuga Perumal, and M. Mohamed Sathik. Image de-noising using discrete wavelet transform. *International Journal of Computer Science and Network Security*, 8(1), January 2008.

[19] R. R. Coifman and D. L. Donoho. Translation-invariant de-noising. In *Wavelets and Statistics, Springer Lecture Notes in Statistics 103*, pages 125–150, 1994.

[20] J. P. Egan. Signal detection theory and roc analysis. *Academic Press*, 1975.

[21] R. Singh, M. Vatsa, A. Noore, and S. K. Singh. Age transformation for improving face recognition performance. In *Pattern Recognition and Machine Intelligence (PReMI)*, pages 576–583, November 2007.