MVA2005 IAPR Conference on Machine VIsion Applications, May 16-18, 2005 Tsukuba Science City, Japan

11-5

JPEG Compression Effects on a Smart Card Face Verification System

Thirimachos Bourlai Josef Kittler Kieron Messer
University of Surrey, CVSSP Group, Guildford, GU2 7XH, U.K
{t.bourlai, j.kittler, k.messer}@surrey.ac.uk

Abstract

We discuss the effect of a compression scheme to be applied to image data in a smart card based face verification system. Accordingly, we propose a system architecture considering trade-off between performance versus the improvement of memory and bandwidth management. In order to establish the system limitations, studies were performed on BANCA, XM2VTS and FERET databases demonstrating that by using JPEG compression on face representations, the verification performance of the system is not degraded and that the proposed architecture is a viable one allowing also the possibility of non-optimum selection of normalisation parameters in the preprocessing stage. Different results were achieved on different databases, indicating that the use of different operating scenarios for system evaluation may call for different optimum operating points.

1. Introduction

Face recognition is an advancing technology and many researchers are contributing their work in different fields of the subject. However, direct comparison of the reported methods [10, 6] can be difficult because testing is performed on different data with variations in the model database sizes and evaluation protocols. Moreover, the viewing conditions, illumination and background of probe images and at the same time the representation of template images, varies considerably on different systems. Therefore, it is difficult to decide on the best method and the appropriate scenario to be used. Important issues are also the computational needs of these methods and the representation capacity of such systems.

Developers in the field require that face representations can be transmitted in the minimum of time and take up as little space as possible. These requirements call for efficient image compression algorithms, especially for embedded applications where dedicated hardware is often employed. Smart cards are such an example that can support a reliable and secure storage for biometric templates. In the distributed architecture proposed [2] the biometric verification is incorporated on the smart card. A novel face verification technique was used [4] in order to limit the face image representation and at the same time to achieve satisfactory verification performance, whilst making the best of the available smart card resources (CPU, storage capacity, bandwidth).

However, a pertinent question is what trade-off between performance and computational time is acceptable, and whether there are parameters that should be investigated. The answer to the latter question is affirmative, because in a real time application that uses a small platform for transfer and storage of facial representations, a developer has to suggest an architecture considering the improvement of memory and bandwidth management versus performance. In our case, this has been achieved to a certain level by keeping the grey level resolution of the normalised probe images on the server unaffected, by reducing the spatial resolution of those images and the biometric templates stored on the card and by using fixed point arithmetic to reduce the bit resolution of the mathematical operations[3]. A further boost in the efficiency of the verification process can be realized by incorporating an appropriate image compression method for still images in the various stages of the process used for creating face representation. In order to use the more efficient compression method for such a system, the main factors that have been considered are compression ratio, computational complexity, compatibility, scalability, memory management and data type dependence. Therefore, the selection of JPEG came up because in addition to being an international standard, it makes a claim to high visual fidelity, satisfactory error resilience, generality (the ability to efficiently compress different types of imagery across a wide range of bit rates) and last but not least, it achieves one of the lowest complexities compared to the methods like JPEG2000. Among many JPEG compression schemes, the baseline mode based on the *Discrete Cosine Transform* (DCT) was used, which ensures compatibility at low quality values and it is very easy to implement and adopt on a small platform while achieving high compression/decompression speed.

In this paper we revisit the performance versus computational complexity trade-off concerns and propose the use of JPEG within different stages of the verification process in our novel distributed architecture at a number of quality settings of the compressor. Image quality is traded off against file size by adjusting these settings. In order to establish the limitations of such a system we investigate the effect of JPEG compression on either the probe and template 8bpp gray level images. We show that system performance is dependent on the database used to perform the experiments. It will be demonstrated that the use of image compression using JPEG coder/decoder, does not necessarily result in performance degradation and may even become advantageous when used to compress probe images, templates or both under specific scenarios.

The rest of the paper is organised as follows. In the next section, the reasons of using JPEG in our proposed smart card face verification system architecture will be presented. In Section 3 the smart card used in our investigation is detailed and its limitations discussed. In Section 4 the experiments made to optimise our system are described. Finally, some conclusions are made.

2. JPEG in our Face Verification System

In any face verification system the user must make an identity claim, usually by the use of a token stored on a smart card. To make a claim, the user presents himself/herself to a camera and places his/her card in the card reader. The token is read off the card and the relevant biometric template retrieved. A match between the template and the acquired image is then made. Prior to this the user would have had to have gone through an enrolment process where their facial biometric template was created and stored in a database and/or on the smart card. The acquired image will typically have to pass through several processing steps before the final matching takes place. These are: face detection/localisation; geometric and photometric normalisation and feature extraction. In our novel architecture, security and privacy is further enhanced when feature extraction and decision making is performed on the smart card. This model is more secure than other proposed architectures (centralised, semi-centralised) because the template is stored and never leaves the smart card. However, smart cards are limited computing devices suffering from restrictions in their specifications. Therefore, it is not yet viable to do all the processing required on the card and it is important to effectively manage its proprietary computation.

Even though the method adopted offers a significant processing relief by reducing the limit of facial representations through the use of client-specific LDA-based method[4], one way of further decreasing the processing overload of our system is by applying a compression scheme on the probe and template images. This would result in a considerable decrease in the representation capacity required for the images to be sent, stored and processed on the card each time we enrol a client or verify a potential client. The selection of the appropriate compression method should be based on the complexity of the compression scheme, which can determine whether a given algorithm is a viable one for the application at hand and whether it best exploits/fits the system specifications. *Compression efficiency* is not the only *complexity measure* in image compression [7] that can determine such a selection, especially in the case where a smart card is being used to perform real time enrolment/verification and requiring the minimum computational power for encoding and decoding.

Other measures are considered to be *memory capital* (the amount of memory needed to execute an algorithm),*memory bandwidth* (the number of times the data must be accessed to perform the algorithm), *total working memory*, *number of CPU cycles*, *number of arithmetic operations* and finally, *the difficulty of implementation of the algorithm*.

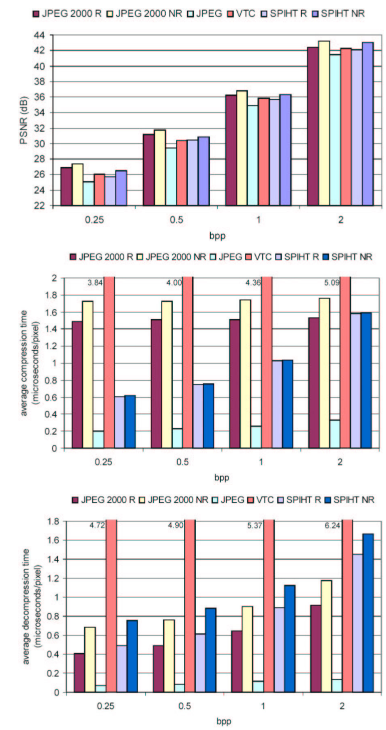

Figure 1. Overall results for non-progressive lossy compression, including encoding and decoding times [9]

In this paper, in order to prove that JPEG was the most appropriate selection for our experiments, we considered the evaluation study on the comparison between different still image coding standards [8]. The results of this work show that the choice of the 'best' standard is application dependent. In particular, even though JPEG2000 offers the richest set of features and provides superior rate-distortion performance, this comes at the price of additional complexity when compared to JPEG. In the cases where lossy compression is of interest and low complexity of high priority, JPEG provides a satisfactory solution. Additional information about the comparison of different -non-progressive lossy compression methods (JPEG2000, JPEG, VTC, SPIHT) can be found in [9]. JPEG2000 was used in its default options; JPEG was used in its baseline mode with flat quantisation tables and optimised Huffman tables.

In some of the results presented in *figure 1* reproduced from reference [9], we can see the benefit of using JPEG. Although JPEG exhibits a considerable quality difference at all bit rates when compared to other methods, it outperforms them in the encoding and decoding times. Therefore, by adopting this scheme we can expect compression of the storage capacity volume of our face database and of the template stored on the card; speed up of the enrolment and verification process, because the coded versions of templates (probes) will be sent, stored and decompressed on the card.

3. The Smart Card

The smart card used for this research was provided by Sharp Laboratories, Oxford, UK. It boasts a 13.5MHz processor, 1Mbyte of EEPROM, 8Kbytes of RAM, a cryptographic co-processor and operates in both contact and contactless modes. In order to perform the necessary on-card verification experiments we used it in a contact mode, which has a data transfer rate of 76.8Kbits per second. It does not have a floating point co-processor, which makes complex mathematical calculations computationally expensive. Also, the data transmission rate between the server and card is fairly slow. Therefore, the amount of data being exchanged between a smart card and a server through an interface (e.g. a biometric template or a facial image) must be kept to a minimum. Finally, the amount of RAM available on the smart card is limited, which means all the data can not be kept in memory for the calculations and the ROM must be used as a cache. Typically, reading data from the EEPROM is fairly fast but writing data is slow.

4. Experimental Setup and Results

Our face verification system has been evaluated via a set of experiments using XM2VTS[5], BANCA[1] and FERET data sets in a total of eight different testing configurations:

- XM2VTS C1, C2: Configuration I and II for the XM2VTS database.
- FE-XM2VTS C1, C2: Configuration I and II for the XM2VTS database but with FERET data set used to generate the initial statistical model.
- BANCA(P, G): P and G protocol for the BANCA database.
- FE-BANCA(P, G): P and G protocol for the BANCA database but with FERET data set used to generate the initial statistical model.

Te original resolution of the image data was 720x576. The experiments were performed with a relatively low resolution face images, namely 55x51 (used as a reference for our study). Also, a JPEG library was used as a part of the Independent JPEG Group software, which has the additional feature that it ensures compatibility at low bit rates. Among many JPEG coders, sequential JPEG was selected because it is the simplest to implement, fastest to execute and easiest to be ported on a small platform.

We investigated the effect of using JPEG compression at four different main scenarios (operational stags):

1. On probe images of all experimental sets, training, evaluation and testing set;
2. On probe images of only evaluation and testing set. This was deliberately chosen because it would be interesting to witness the effect of compression on the overall performance only in the case where probe images are sent to the smart card and training remains unaffected;
3. On templates;
4. On both probes (training and testing) and templates.

Different quality settings for the compressor were used. Image quality was traded off against file size by adjusting those settings. In all cases, the range of the quality factor was modified from 5 to 100. In order to identify the optimum JPEG scenario, the system was evaluated across all scenarios and databases used by measuring the performance levels of the verification system (FA, FR and Half Total Error Rates) on the test set. However, we also took into consideration the comparison between the initial HTER and the average HTER for all quality values (5-100) and the the consistency of the good performance results in each JPEG scenario.

By observing the face representations across all quality range we concluded that even at the lowest quality, where cubist effects are introduced, images still retain their discriminative structure. Interestingly, the results achieved on

Table 1. Best cases for all databases (PROT=Protocol, PR=Probes, TE=Templates, Tr=Train, Te=Test)

DATABASES	PROT	Case	QUAL	COMPR	HTER old	HTER new
XM2VTS	CI	PR/Tr/Te	7.5	5.11:1	0.0458	0.0417
XM2VTS	CII	PR/Tr/Te	10	4.58:1	0.0264	0.022
FERET-XM2VTS	CI	PR/Te	15	4.11:1	0.0602	0.05939
FERET-XM2VTS	CII	PR/Te	70	2.28:1	0.037	0.03483
BANCA	P	PR/Tr/Te	25	3.51:1	0.184	0.17261
BANCA	G	PR/Tr/Te	35	3.13:1	0.0629	0.06122
FERET-BANCA	P	PR/Te	80	1.94:1	0.277	0.2621
FERET-BANCA	G	TE	50	2.76:1	0.12	0.1179

the BANCA and XM2VTS databases (even when FERET was used for training) were comparable (*see Table 1*). XM2VTS is more consistent in achieving overall slightly better performance results than when no JPEG was used, especially in the case when all probe images were compressed in both the training and testing sets. BANCA behaved accordingly and because of its database size, proved to be more sensitive in the overall performance. The best performance was gained in the case of protocol P, which better represents the actual system performance (client training in 1 controlled session and client and impostor testing from all condition sessions). Using FERET for training and XM2VTS for testing, the system behaved almost the same. However, with BANCA used for testing the results were in total worse across all cases, proving that database size and the use of compression on a different set for training can significantly affect the system performance. Some representative cases are presented in *figure 2*.

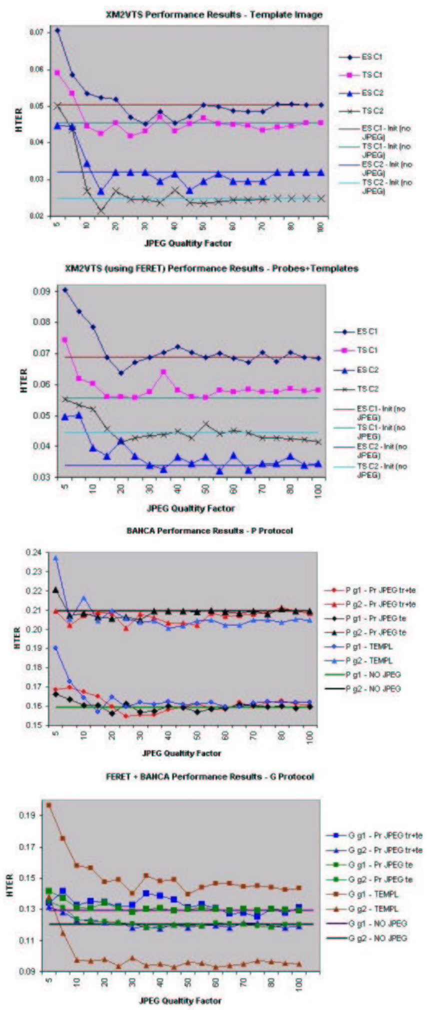

Figure 2. Selected cases of the DBs used

5. Discussion and Conclusions

Proposing an optimised smart card face verification system design in terms of performance and memory management is a very complex process, with many key factors to consider. A designer has to suggest an optimum operating point in terms of the overall system speed versus the performance requirements, when using different data types, gray-levels and spatial image resolutions for the face representations. However, this specification can be further changed to our benefit when a certain compression scheme is applied to our system. In such a distributed architecture not only can we offer increased security and privacy in comparison with conventional architectures, but improved memory management without performance deterioration. The significance of compression can be further appreciated when fusion methods are to be incorporated onto the smart card and therefore an increased number of biometric templates has to be stored on the card.

Experiments showed that in order to optimise the smart card design, a potential JPEG quality factor should be selected, which is scenario and database dependent. Below this quality threshold, the performance can degrade. Above that, there is a surprisingly wide quality range where compression does not seem adversely to affect performance, and for specific scenarios it may even improve system performance. Generally speaking, when operating at the limit of the quality settings we can achieve good performance as well as gain in memory size and transfer speed. For instance, in XM2VTS for a quality factor of 7.5 we have an improvement in performance of 14% and achieve image compression of more than 5 to 1 (*see table 1*).

Acknowledgements

The authors would like to acknowledge the support received from OmniPerception Ltd, Sharp Laboratories, U.K and EPSRC under grant GR/S46543/01(P).

References

[1] E. Bailly-Baillire, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariethoz, J. Matas, K. Messer, V. Popovici, F. Poree, B. Ruiz, and J.-P. Thiran. The banca database and evaluation protocol. *AVBRA*, 2003.

[2] T. Bourlai, K. Messer, and J. Kittler. Face verification system architecture using smart cards. *ICPR 2004*, 23-26 August 2004.

[3] T. Bourlai, K. Messer, and J. Kittler. Performance versus computational complexity trade-off in face verification. *ICBA 2004*, 15-17 July 2004.

[4] Y. Li, J. Kittler, and J. Matas. Face verification using client specific fisher faces. *In J. T. Kent and R. G. Aykroyd, editors, Proc. Int. conf. on The Statistics of Directions, Shapes and Images*, pages 63–66, September 2000.

[5] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre. Xm2vtsdb: The extended m2vts database. *AVBRA*, pages 72–77, March 1999.

[6] P. J. Phillips, M. McCabe, and R. Chellappa. Biometric image processing and recognition. *EUSIPCO*, 1998.

[7] J. Reichel. Phd thesis no 2326:. *Polytechnic University of Lausanne, Switzerland*, 2001.

[8] D. Santa-Crus and T. Ebrahimi. A study of jpeg 2000 still image coding versus other standards. *In Proc. Of the X European Signal Processing Conference, Signal Processing Laboratory, Swiss Federal Institute of Technology, Lausanne*, pages 673–676, September 2002.

[9] D. Santa Cruz and T. Ebrahimi. A study of jpeg 2000 still image coding versus other standards. *ESPC*, 2:673–676, September 2000.

[10] W. Zhao, R. Chellappa, A. Rosenfeld, and P. Phillips. Face recognition: A literature survey. *UMD CfAR Technical Report CAR-TR-948*, 2000.