SECURITY ALGORITHM OF FACE RECOGNITION BASED ON LOCAL BINARY PATTERN AND RANDOM PROJECTION

Zhou Lingli [1], Lai Jianghuang [2*]

[1]School of Mathematics and Computational Science, Sun Yat-Sen University, Guangzhou 510275
[2]School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275

ABSTRACT

With the growing applications of biometrics, there are many concerns about the security and privacy of the biometrics data. This paper proposes a security algorithm of face recognition, which bases on the local binary pattern (*LBP)* and random projection. Feature extraction is first performed on face images by *LBP* operator. Random projection is done using the random matrix which is generated by user specific key. All the above successive procedures produce the cancelable and non-invertible feature data, which is stored in template databases and can achieve the protection of biometrics data. In extensive experiments with publicly available face datasets *ORL*, *YALE* and *FERET*, higher recognition accuracy is reached, which demonstrates that the proposed approach is able to not only protect the biometrics data, but also is robust to various complex conditions, such as illumination, changes in the pose and expression, etc.

Index Terms—biometric recognition, cancelable biometric, biometric cryptosystem, *LBP*, random projection

1. INTRODUCTION

Biometrics, described as the science of recognizing an individual based on his or her physical or behavioral traits has began to gain acceptance as a legitimate method to identify individuals [1]. With the deployment of biometrics, there are growing concerns about privacy invasion and data security [2].

Unfortunately, biometric technology has some inherent limitations and uncertainties. Such as, the data is permanently associated with the subject and it can't be revoked or cancelled [3]. The biometric is not secure because biometric information can be recorded or misused without a user's consent. The biometric characteristic of everyone is limited, such as everyone has only one face and ten fingers. The template in biometrics system stores the biometrics which is extracted from the authenticated person. Using "Hill Climbing Attack"[4]can regenerate a face image from a face template. Template security is an important consideration and concern multiplies when template information is shared among commercial organization.

The template protection technologies can be broadly classified into two categories, namely, cancelable biometric approach and biometric cryptosystem.

The cancelable biometric [1] approach stores an irreversibly transformed version of the biometric template, instead of the original biometric. With different parameters, a new template can be reproduced then matching is performed in a transformed domain. The parameters of the transformation function are typically derived from a random key or password which is unrelated with the biometrics data. Savvides *et al*. [5] introduced a scheme which encrypted the training images used to synthesize the correlation filter for face authentication. Ratha *et al*. [6] proposed and analyzed three non-invertible transforms for generating cancelable fingerprint templates. The three transformation functions are Cartesian, polar and functional. Teoh *et al*. [7] proposed Biohashing algorithm which combines randomized token and biometric data to generate a set of user-specific compact codes. Teoh *et al*. [8] introduced Biophasor as a form of cancellable biometrics.

Uludag *et al*. [2] proposed biometric cryptosystem which aimed at integrating the cryptographic technique into a biometric system. Some public information about the biometric template is stored in the biometric cryptosystem. This public information is usually referred to as helper data. While the helper data does not reveal any significant information about the original biometric template, it is needed during matching procedure to extract a cryptographic key from the query biometric features. Matching procedure is performed indirectly by verifying the validity of the extracted key. Error correction coding techniques are typically used to handle intra-user variations. Juels *et al*. [9] proposed fuzzy commitment schemes which can tolerate more variation in the biometric characteristics and provide stronger security. Juels *et al*. [10] introduced fuzzy vault scheme which unlike the fuzzy commitment schemes does not require the biometric representations to be ordered. Feng *et al*. [11] proposed a hybrid approach which combined the

* Correspondence Author: stsljh@mail.sysu.edu.cn. The project is supported by NSFC (60675016, 6033030), 973 Program (2006CB303104) and NSFC-GuangDong United Project (U0835005)

Proc. 9th IEEE Int. Conf. on Cognitive Informatics (ICCI'10)
F. Sun, Y. Wang, J. Lu, B. Zhang, W. Kinsner & L.A. Zadeh (Eds.)
978-1-4244-8040-1/10/$26.00 ©2010 IEEE

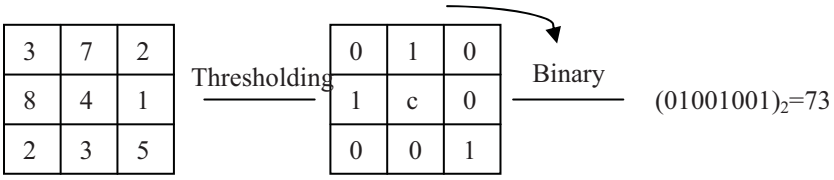

Fig.1. Illustration of original *LBP* operator

cancellable biometric approach and biometric cryptosystem.

Now, most researches about template security are about fingerprint and iris. The template security of face is seldom mentioned. Face feature has large intra-class invariant because of changing of illumination, expression and pose. Comparing with iris and fingerprint recognition, face recognition has merits of nature and not be detected by individual. Face recognition has various applications in automated surveillance, information security, automatic access control. Considering all above, we propose a security algorithm to protect face template, which bases on the *LBP* and random projection.

The rest of this paper is organized as follows: Local Binary Pattern (*LBP*) is briefly introduced in Section 2. In Section 3, Random projection is presented in detail. Our proposed security algorithm of face recognition based on *LBP* and random projection is presented in Section 4. The extensive experimental results with publicly available face datasets *ORL*, *YALE*, *FERET* and comparison with Biohashing algorithm are presented in detail in Section 5. Finally, the conclusion is given in Section 6.

2. LOCAL BINARY PATTERN

The ordinary *LBP* operator, introduced by Ojala [12], is becoming very popular in pattern recognition. The operator labels the pixels of an image by thresholding the 3*3 neighborhood of each pixel with the center pixel. An illustration of original *LBP* operator is shown in Fig.1. *LBP* operator with any radius *R* and the number of neighboring pixels *P* is allowed by using circular neighborhoods and bilinear interpolation technique as described in [13], denoted by $LBP_{P,R}$.

We defined the local neighborhood of a pixel

$$T = t(g_c, g_0, \cdots, g_{P-1}) \tag{1}$$

where g_c is the grey value of central pixel and $g_i (i = 0, \cdots, P-1)$ correspond to *P* number of neighbor's grey value.

Abstracting the g_c from g_i :

$$T = t(g_c, g_0 - g_c, \cdots, g_{P-1} - g_c) \tag{2}$$

To get grey-scale variance, thresholding the neighbor pixels with the center can be presented as

$$T = t(s(g_0 - g_c), \cdots, s(g_{P-1} - g_c)) \tag{3}$$

where $s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$.

To assign a weight 2^i to each $s(g_i - g_c)$, the results can be written in Eq.4.

$$LBP_{P,R} = \sum_{i=0}^{P-1} s(g_i - g_c) \cdot 2^i \tag{4}$$

Another two extensions of *LBP* operator are uniform version $LBP_{P,R}^{u2}$ and rotate invariant version $LBP_{P,R}^{ri}$ [13]. *LBP* is defined as uniform if it contains at most two bitwise 0 to 1 or 1 to 0 transitions, that is to say, the following condition must be satisfied:

$$|s(g_{P-1} - g_c) - s(g_0 - g_c)| + \sum_{i=1}^{P-1} |s(g_i - g_c) - s(g_{i-1} - g_c)| \leq 2 \tag{5}$$

$LBP_{P,R}^{ri}$ is done with a bit-shift operator where the code is circularly shifted until its minimum

$$LBP_{P,R}^{ri} = \min(ROR(LBP_{P,R}, i) | i = 0,1,..., P-1\} \tag{6}$$

Uniform and rotation invariant are often combined to generate $LBP_{P,R}^{riu2}$ to make the *LBP* operator more statistically strong and get shorter codes with minimum information loss. It is noted $LBP_{P,R}^{riu2}$ reduces the number of possible patterns from 2^P to *P+1*, and the length of *LBP* histogram is only related to the number of neighboring points *P*.

For image recognition, the image is divided into some rectangular regions and *LBP* descriptors are extracted from each region independently. The *LBP* descriptors are then concatenated to form an image.

Several possible dissimilarity measures have been proposed for histograms:

(1) Histogram intersection:

$$D(S, M) = \sum_i \min(S_i, M_i) \tag{7}$$

(2) Log-likelihood statistic:

$$L(S, M) = -\sum_i S_i \log M_i \tag{8}$$

(3) Chi square statistic(χ^2):

$$\chi^2(S, M) = \sum_i \frac{(S_i - M_i)^2}{S_i + M_i} \tag{9}$$

Due to its statistics property and low computational cost, *LBP* has proven to be powerful in face, texture and dynamic

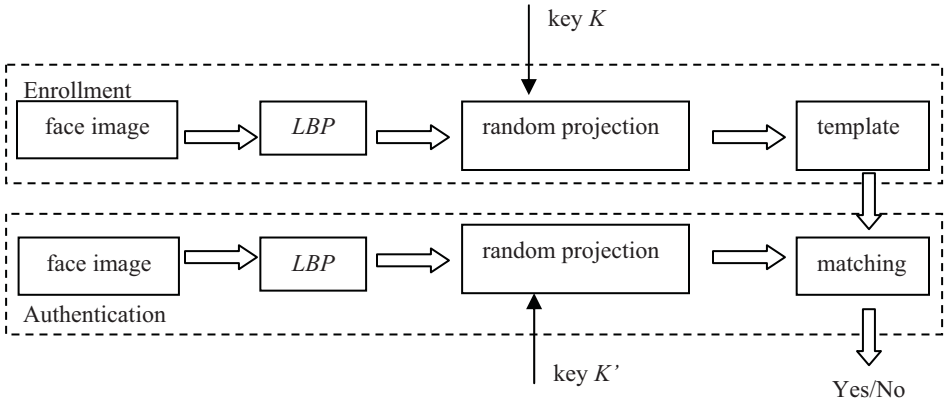

Fig. 2. Description of our approach

texture description. Inspired by these successful applications, we consider exploiting $LBP^{u2}_{P,R}$ to extract face feature and using Chi square statistic as dissimilarity measures.

3. RANDOM PROJECTION

Random projection is proposed by Johnson and Lindenstrauss [14]. Comparing to other dimensionality reduction technology such as *PCA*, random projection [15] is an effective and accurate approach. Despite the computational simplicity of random projection, it does not introduce a significant distortion in the data.

The key idea of random projection arises from the *Johnson-Lindenstrauss* lemma [14] which is to map a set of vectors into a new space, while the Euclidean distance between these vectors are barely changed after transform. Lemma 3.1 is proved.

Lemma 3.1 (Johnson-Lindenstrauss) Give $0 < \varepsilon < 1$ and an integer *N*, let *d* be a positive integer such that $d \geq d_0 = O(\varepsilon^{-2} \log N)$. For every set P of *N* points in R^s there exists $f : R^s \to R^d$ such that for all $u, v \in P$,

$$(1-\varepsilon)\|u-v\|^2 \leq \|f(u)-f(v)\|^2 \leq (1+\varepsilon)\|u-v\|^2 \quad (10)$$

In a random projection, original *n*-dimensional data is projected to a *d*-dimensional subspace though a $d \times n$ random matrix $R_{d\times n}$:

$$X^{RP}_{d\times M} = R_{d\times n} X_{n\times M} \quad (11)$$

The key factors of random projection are random matrix $R_{d\times n}$ and the subspace dimension *d*. The random matrix $R_{d\times n}$ can be calculated using the following algorithm:

(1) Set each entry of $d \times n$ random matrix to an i.i.d. *N*(0,1) value.

(2) Orthogonalize the *d* rows of the matrix using the Gram-Schmidt algorithm.

(3) Normalize the rows of the matrix to unit length.

4. SECURITY ALGORITHM BASED ON *LBP* AND RANDOM PROJECTION

The description of our proposed security algorithm of face recognition is shown in Fig.2, which has two steps.

(1) To extract the face feature from face image using *LBP* operator.

Most existing approaches about template data usually extract global feature such as *LDA*, *PCA*. There are others approach of feature extraction [16][17][18][19]. These global features are sensitive to different expression, illumination, pose among the same person's different images, and influent the recognition results.

LBP operator considers both shape and texture information to represent the face images. Our experimental results show that *LBP* feature is robust with respect to facial expression, aging, illumination and makes some improvements of recognition results.

(2) To make random projection with *LBP* face features.

The original *n*-dimensional *LBP* feature data is projected to a *d*-dimensional subspace $X^{RP}_{d\times M} = R_{d\times n} X_{n\times M}$, where $R_{d\times n}$ is a $d \times n$ random matrix, $X^{RP}_{d\times M}$ is the projected d-dimensional feature. Through the random projection, the features template stores $X^{RP}_{d\times M}$, not $X_{n\times M}$. The matching procedure is performed between $X^{RP}_{d\times M}$.

Random matrix $R_{d\times n}$ is generated by random number generator which is controlled by user key *K*. Every user has different key. The key of lawful holder can only decide the generation of random matrix. In enrollment and authentication phase, random projection is conducted by the same way with different key.

Random projection is closely related to the key *K*. With different keys, a new template data can be reproduced. With random projection, the data in template is cancelable and the user's privacy is protected.

Random projection $X^{RP}_{d\times M} = R_{d\times n} X_{n\times M}$ is an underdetermined equation because $d << n$. This is a many-

to-one projection and it is non-invertible, that is, when $X_{d\times M}^{RP}$ and $R_{d\times n}$ are stolen, but the original feature data $X_{n\times M}$ is safe. It guarantees the safety of original data. In authentication phase, the user only can be recognition correctly with the correct feature data and correct key.

5. EXPERIMENTAL RESULTS

5.1. Evaluation dataset

Our proposed security algorithm is conducted in *ORL*, *YALE* and *FERET* face database. The *ORL* database is made up of 400 images, 10 each of 40 persons. The face images of a same person have different expression. The *YALE* dataset consists of 15 individuals' images. There are 11 images per person. The face images have changing of illumination and expression. The *FERET* database contains over 1000 images from 255 persons. The face images of a same person have different illumination, pose and expression.

5.2. Experimental analysis

In T.Ahonen's experiments [20], $LBP_{8,2}^{u2}$ and Chi square statistic are more appropriate for face recognition. In our method, the face recognition is performed a nearest neighbor classifier in the computed feature space with χ^2 as a dissimilarity measure. The *LBP* operator is $LBP_{8,2}^{u2}$, so the histogram length is 59 (8*(8-1)+3). In order to reduce the randomness influence, the experiments are executed for cycling five times and mean recognition rate is obtained.

In reality face recognition, the face is first divided into rectangular regions and $LBP_{8,2}^{u2}$ descriptors are extracted from each region independently. The $LBP_{8,2}^{u2}$ descriptors are then concatenated to form an image. In our experiments, the face is all divided into 3*3 rectangular regions. The face images in *ORL* and *FERET* database is divided into 9 rectangular regions with 30*37 pixels. The face images in *YALE* database is divided into 9 rectangular regions with 43*43 pixels. Length of feature vector is 531(59*9). Table.1 denotes the recognition rate with $LBP_{8,2}^{u2}$ and χ^2.

Face database	*ORL*	*YALE*	*FERET*
Recognition rate	0.93	0.66	0.72

Table.1. Recognition rate with $LBP_{8,2}^{u2}$ and χ^2

When the user has true key($K = K'$), the recognition rates of *ORL*，*YALE*，*FERET* database are shown in fig.3–fig.5. Comparing with the Table.1, it noted that the performance of our proposed method significantly increases the recognition rate.

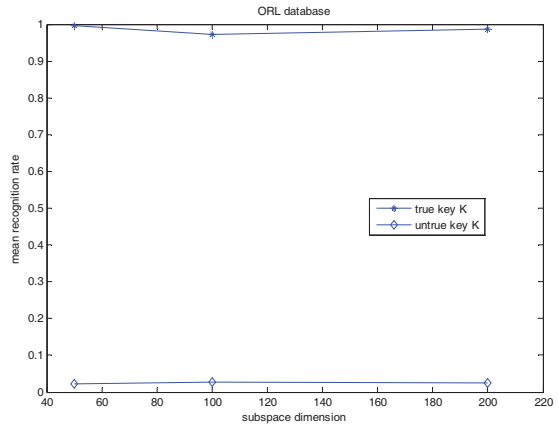

Fig.3. Recognition rate of *ORL* database

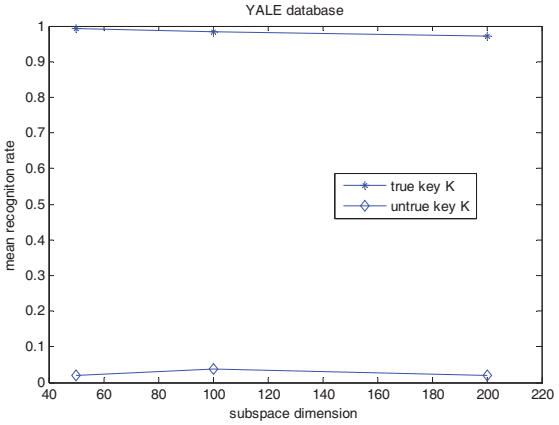

Fig.4. Recognition rate of *YALE* database

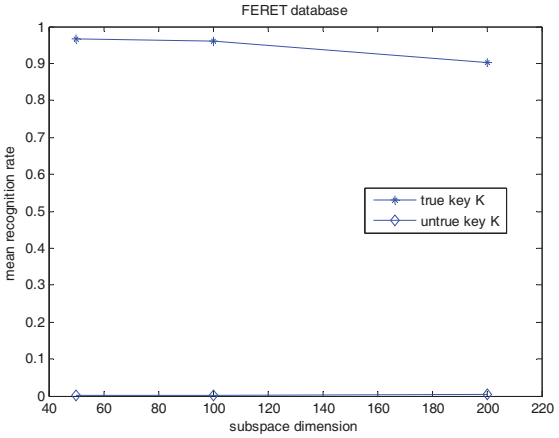

Fig.5. Recognition rate of *FERET* database

The variations of illumination, pose and expression in *YALE*, *FERET* database are more violently than that of *ORL*

Subspace dimension	*ORL* (160)		*YALE* (60)		*FERET* (255)	
	LBP+RP	Biohashing	*LBP+RP*	Biohashing	*LBP+RP*	Biohashing
50	0.022	0.025	0.019	0.051	0.001	0.004
100	0.028	0.029	0.038	—	0.002	0.003
200	0.024	0.032	0.021	—	0.003	0.006

Table.2. Algorithm comparison

database. The recognition rates of *YALE*, *FERET* database are lower than that of *ORL* database in table.1. But in fig.3-fig.5, the results of *YALE*, *FERET* database increases than these of Table.1. It is denoted that our proposed method is quite robust with respect to the variation of illumination, pose and expression.

When the user doesn't own true key ($K \neq K'$), the recognition rates of *ORL*, *YALE*, *FERET* database are also presented in fig.3-fig.5. The experimental results show the recognition rates are very lower. It is indicated that our proposed approach has high security.

In random projection, the subspace dimension *d* is a key factor. To analyze the influence of *d*, its value is 50, 100, 200 respectively in our experiments. It shows that the recognition rates vary very little in Fig.3-Fig.5. Therefore, our security algorithm is robust of subspace dimension.

5.3. Algorithm comparison

Teoh [7] proposed Biohashing algorithm based on iterative inner products between feature vectors and random sequences. In this way a set of user-special compact codes can be produced, which is named BioHashCode. Using Hamming distance as dissimilarity measures between BioHashCode. Biohashing algorithm has higher recognition rate with true key. But its recognition rate is lower than our proposed method.

Table.2 presented the recognition rates of *ORL*, *YALE*, *FERET* database when the user hasn't true key. In this case, the recognition is the lower the better. The biometric system must reject the user who hasn't legal key. In Table.2, the "*LBP+RP*" denotes our proposed algorithm. The number after database's name represents the dimension of feature vector in Biohashing algorithm which is obtained by some feature extraction algorithm (*PCA*, *LDA*). The dimension of feature vector is 60 in *YALE* database, so it can't execute the experiments with subspace dimension 100 and 200.

In Table.2, recognition rate of *ORL* dataset has little difference. But recognition rate of our algorithm decreases much in *YALE*, *FERET* database. Thus it is demonstrated the using *LBP* to extract feature can reduce the impact of variant of illumination, pose and expression. Furthermore, our proposed algorithm is robust with the variant of illumination, pose and expression.

6. CONCLUSION

With the explosion in the need to employ human authentication, there is growing concern about the security and privacy of biometrics. This paper proposes a security algorithm which produces cancellable and non-invertible about face template data. Feature extraction is first performed on face images by *LBP* operator. Random projection is done using the random matrix which is generated by user specific key. All the above successive procedures, it can achieve the protection of biometric data. Experimental results show our algorithm is able to not only protect the biometric data, but also is robust to various complex conditions, such as illumination, pose and expression, etc.

REFERENCES

[1]N.K. Ratha, J.H. Connell and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication system," *IBM Sys. J.*, vol.40, no.3, pp.614-634, 2001.

[2]U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, "Biometric cryptosystems: issues and challenges," *Proc of the IEEE*, vol.92, no.6, pp. 948-960, 2004.

[3]Bruce Schneier, "Inside risks: The uses and abuses of biometrics," *Com. Of the ACM*, vol.42, pp.136, 1999.

[4]A. Adler, "Images can be regenerated from quantized biometric match score data," *Proc of Canadian conference of Electrical and Computer Engineering*, pp. 469-472, 2004.

[5]M. Savvides, B.V.K. Vijaya Kumar and P.K. Khosla, "Cancelable biometric filters for face recognition," *Proc. Int'l Conf. Pattern Recognition*, pp. 922-925, 2004.

[6]N.K. Ratha, S. Chikkerur and J.H. Connell, "Generating cancelable fingerprint templates," *IEEE Trans. on PAMI*, vol.29, no.4, pp. 563-564, 2007.

[7]A.B.J. Teoh, A. Goh and D.C.L. Ngo, "Random multispace quantization as an analytic mechanism for

BioHashing of biometric and random identity inputs," *IEEE Trans. on PAMI*, vol.28, no.12, pp. 1892–1901, 2006.

[8]A.B.J. Teoh, Kar-Ann Toh and Wai Kuan Yip, "2^N Discretisation of BioPhasor in Cancellable Biometrics," *ICB 2007*, pp. 435-444, 2007.

[9]A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Proc. of 6th ACM Conference on Computer and Communications Security*, Singapore, pp. 28–36, 1999.

[10]A. Juels and M. Sudan, "A fuzzy vault scheme," *Proc. of IEEE International Symposium on Information Theory*, pp.408, 2002.

[11]Y.C. Feng, P.C. Yuen and A.K. Jain, "A hybrid approach for face template protection," *Proc. of SPIE Conference of Biometric Technology for Human Identification*, 2008.

[12]T. Ojala, M. Pietikainen and D. Harwood, "A comparative study of texture measures with classification based on feature distribution," *Pattern Recognition*, vol.19, pp. 51-59, 1996.

[13]T. Ojala, M. Pietikainen and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Trans. on PAMI*, vol.24, no.7, pp. 971-987, 2002.

[14]W.B. Johnson, J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," *Conference in modern analysis and probability*, vol.26 of Contemporary Mathematics, pp.189-206, Amer. Math. Soc.,1984.

[15]N. Goel, G. Bebis and A. Nefian, "Face recognition experiments with random projection," *SPIE Defense and Security Symposium*, 2005.

[16]Frank Y. Shih, Chao-Fa Chuang and Patrick S. P. Wang, "Performance comparisons of facial expression recognition in JAFFE database," *International Journal of Pattern Recognition and Artificial Intelligence,* pp. 445-459, 2008.

[17]Sang-Woong Lee, Patrick S. P. Wang, Svetlana N. Yanushkevich and Seong-Whan Lee, "Noniterative 3D face reconstruction based on photometric stereo," *International Journal of Pattern Recognition and Artificial Intelligence,* pp. 389-410, 2008.

[18]Frank Y. Shih, Shouxian Cheng, Chao-Fa Chuang and Patrick S. P. Wang, "Extracting faces and facial features from color images," *International Journal of Pattern Recognition and Artificial Intelligence*, pp.515-534, 2008.

[19]Xinge You, Qiuhui Chen, Patrick Wang and Dan Zhang, "Nontensor-Product-Wavelet-Based Facial Feature Representation," *Image Pattern Recognition- Synthesis and Analysis in Biometrics, WSP* 2007.

[20]T. Ahonen, A. Hadid and M. Pietikainen, "Face recognition with local binary patterns," *The 8th European Conference on Computer Vision*, Springer, 2004.