ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/1513
DOI URL: http://dx.doi.org/10.21474/IJAR01/1513

RESEARCH ARTICLE

PRIVACY PROTECTED FACE VERIFICATION SYSTEM USING SPARSE CLASSIFIER.

Thasni A N and Deepthi V R
Department of Computer Science and Engineering, RIT, Kottayam, India.

Manuscript Info

Manuscript History

Received: 12 July 2016
Final Accepted: 19 August 2016
Published: September 2016

Key words:-
face scrambling; SIFT; LBP; T-test; Sparse Representation classifier.

Abstract

The demand of video surveillance has been increasing day by day; as a result the privacy protection has become a responsibility for the public as well as for legal authorities. When videos are transmitted or distributed across various public networks, the human faces should not be exposed. To deal with this problem, facial image scrambling technique appeared as a solution for privacy related applications. This paper proposes a facial verification system in the scrambled domain using sparse classifier. In the proposed method, the facial features are extracted from the scrambled faces using SIFT and LBP feature extraction methods and a T-test based feature selection method is used to select important features for classification. Then sparse representation based classifier is used for classifying the facial images. The experiments show that the proposed face verification system can meet the challenging tests in the scrambled domain.

Introduction:-

Today visual surveillance has become an extensively used technology in various applications. Exposing of face images [1, 2] in the surveillance videos should be avoided when it is transmitting and distributing over different networks. One of the solutions to this problem is the Scrambling technique [3] where the privacy of the subjects can be respected. Image scrambling give more advantages than other methods, it provides lower computational cost and time than encryption method.

Scrambling is a popular method in visual surveillance. It does not really hide anything from surveillance video; it can only avoid exposure of human faces from surveillance videos. This paper uses scrambling of faces using Arnold transform [4, 5]. Using inverse Arnold transform scrambled faces can be recovered easily with different parameters.

There are many scrambling techniques are available. For example, scrambling can be performed by using cartooning techniques [6]. After this method, the faces become extremely hard and it lost the facial information. As a result the face recognition/verification is not performed successfully in this case. So this method is not a good choice for hiding human faces from surveillance video. The Arnold transform [4, 5] differ from all other methods, it is a recoverable type scrambling method and it only change the pixel position. Hence this work uses Arnold transform based scrambling method.

The automatic face verification/recognition is usually a challenging task. Due to this reason face recognition has become a significant research topic in indexing of images [4], human-computer interaction [7~9], forensic biometrics [10] and medical applications [11]. In visual surveillance system, the captured videos are transmitted on

Corresponding Author:- Thasni A N.
Address:- Department of Computer Science and Engineering, RIT, Kottayam, India.

an internet based visual sensor networks. In these situations, the videos are handled by third party servers, where personal privacy needs to be ensured. Further, the storage and distribution of the human faces present in the recorded videos are subjects to legal constraints. As a result face scrambling will be a promising solution to this issue.

This paper proposes a sparse classifier scheme to deal with scrambled facial verification challenge. The sparse classifier scheme is well suited to handle randomly scattered features, and excellent at noise like or chaotic pattern classification. The main advantage of this method is to improve accuracy and reduce time consumption. Experiments are carried out using ORL and Yale dataset.

Related works:-

Face verification or recognition is the one of the prominent research area. There are many methods available for face verification. Now a days privacy is the important thing in the case of human facial images. Number of studies has been proposed for protecting the face images.

Z. Erkin et al. [12] proposed a strong privacy-enhanced face recognition system using secure multiparty computation. This method allows hiding both the server that performs the matching operation and biometrics information. This method is more complex and difficult to implement in encrypted images.

A. Erdlyi et al. [6] proposed a resource-aware cartooning method for privacy protection. Here, the privacy revealing details are removed by converting images into abstracted frames. Cartooning can be applied either to whole images or pre-selected sensitive regions of interest. This method generates “cartoons” it allows recognition but hide the identity of the person in the image. The color filtering and edge enhancements are the two methods for the cartooning. After cartooning the faces lost the facial information. So face recognition become unsuccessful.

Eman A. Abdel-Ghaffar et al. [13] proposes a robust face verification system, which is based on two stage hashing algorithm. It introduces a user dependent one way transformation. Here the keys are generated using modified password-based key derivation algorithm and are not stored in the system database. Furthermore, using encryption as a final stage, it increases the security and overcomes attacks on the communication channels. Encryption has more computational cost and it takes more time. Hence scrambling methods are developed.

A. Melle et al. [3] proposes a pixel domain based reversible scrambling technique. The privacy sensitive ROI is described block wise in a parametric form which exploits the information from the rest of the image. Using a secret key, the encoding parameters are encrypted and stored separately embedded in the image itself by watermarking. The region of interest is decoded by parameters decryption with full or partial knowledge of the secret key, thus leading to different levels of scrambling alteration. Knowledge of the full secret key gives authorized users image recovery at a quality level very close to the original. The visual quality of this method decreases with increasing strength of scrambling. Furthermore, the method brings the face recognition scores down to a level proportional to the strength of scrambling applied.

R. Jiang et al. [14], proposes a secure face verification system in the scrambled domain using fuzzy random forest. The method is partitioned into training and testing stage. In the training stage, faces are scrambled and given to the fuzzy forest learning scheme. This procedure select random feature from the scrambled images with biased weights toward central features. Then construct fuzzy trees based on these selected features. In the testing stage given an image as input, each tree computes a fuzzy membership value and given it to the forest decision process. The forest decision procedure uses Kullback-Lieder divergence method to weighs all the trees. The final decision is based on a combination of all the fuzzy trees. To improve accuracy and reduce time consumption, we introduce a sparse representation classifier to deal with scrambled face verification challenge.

Methodology:-

We proposed a sparse classifier based privacy protected face verification system. The method is carried out in two stages, one is the training stage and other is the testing stage. The training stage determines the feature vector of a set of training images and the testing stage performs robust face verification. SIFT and LBP feature extraction methods are used for feature extraction. Fig 1 shows the flowchart of the methodology.

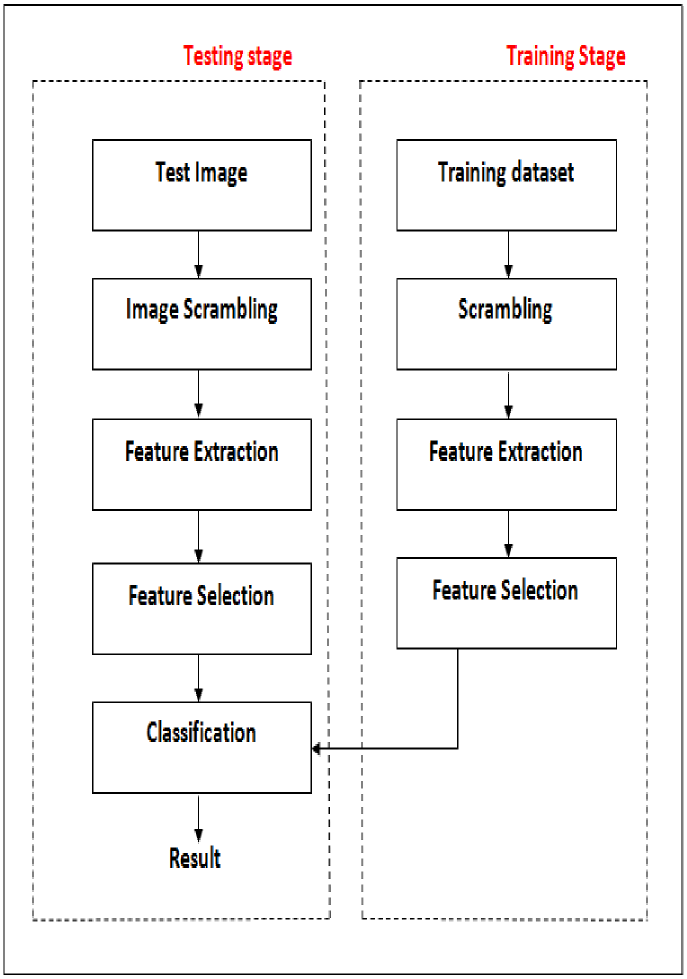


Fig. 1:-Flowchart of the methodology.

Facial image acquisition:-

Images are collected from the Yale database [20]. This database contains fifteen persons and each person's has eleven sample faces. We carried out our face verification experiment using these small dataset by splitting it into training and test dataset. This dataset can be downloaded from http://cvc.yale.edu.

Image scrambling by Arnold Transform:-

Scrambling is the preprocessing step for the training and testing stage. It is like a non-password security algorithm and it hides the information of the image. Digital image scrambling can convert images into irregular and meaningless pattern. After scrambling the images will become irregular pattern like structure, as a result the visual information is hidden from the public eye and privacy is protected even if the visual contents are distributed or browsed over different public network. This work uses Arnold transform based scrambling technique due to its periodicity and simplicity.

In the research of ergodic theory V.I Arnold proposed a method called Arnold transform [4, 5]. It has been called popular image scrambling method due to its simplicity and ease of use. Here we use this method to provide security to the images. In Arnold transform pixel position at (x, y) is transformed to another point (x', y') as follows:

$$\begin{matrix} x' \\ y' \end{matrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{matrix} x \\ y \end{matrix} \bmod N, \qquad (1)$$

This is called two-dimensional Arnold transform. The recursive equation for Arnold transform as follows:

$$P_{xy}^{K+1} = \mathrm{A}P_{xy}^{K} \ , \ \ P_{xy}^{K} = (x,y)^{T} \quad (2)$$

$\mathrm{P}_{\mathrm{xy}}^{\mathrm{K}+1}$ is the output pixel position after K+1th Arnold transform. $\mathrm{P}_{\mathrm{xy}}^{\mathrm{K}}$ is the input pixel position after Kth Arnold transform and A is the transformation matrix. K represents number of iterations, here K= 0, 1 and 2.

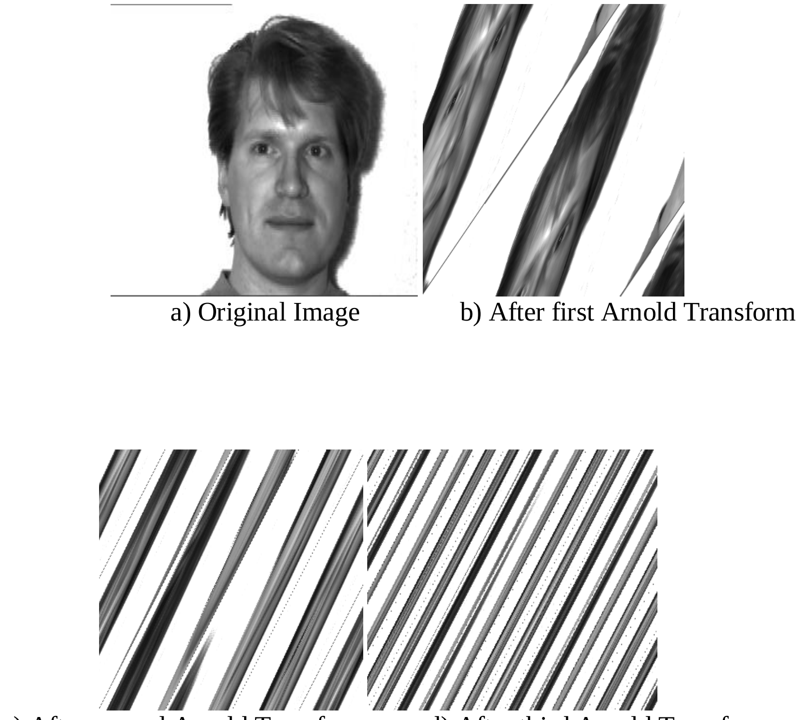
After transformation Arnold transform produce new image and the image is difficult to identify by human eye as show in fig.2. But after transformation the facial information is retained entirely in the image due to the properties of being cyclic and irreversible. Unlike encryption, scrambling process does not really hiding information from the access. It only prevents unwanted exposure of human faces.

Feature Extraction:-

SIFT and LBP feature extraction technique is used for extracting features from the scrambled images.

SIFT Feature Extraction:-

We use SIFT features [16] for face recognition. It is a widely used feature extraction technique which helps matching between same object of different views [17]. The extracted features are unchanged to rotation and scale, and are highly unique of the image. The features are extracted in different steps. In the first step the potential interest points locations are calculated by identifying maxima and minima of a set of Difference of Gaussian (DoG) filters applied at different Scales all over the image. Next step is to discarding low contrast points and refined the location of the potential interest points. Then an orientation is assigned to each keypoint based on local image features. Finally, based on the local image gradient a local feature descriptor is computed at each key point. The feature vector is the 128 dimension vector, which contains the differently identifying neighborhood value around the keypoint.



a) Original Image b) After first Arnold Transform

c) After second Arnold Transform d) After third Arnold Transform

Fig. 2:- Arnold Transform.

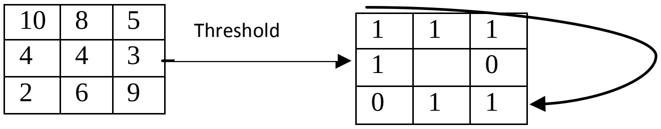
The SIFT features are extracted from all the face images in the training stage. In the testing stage, given a new face image, the extracted features from the image are compared against features in the training set. The nearest face is considered as the face contains largest number of matching points. To reduce the number of false matches, consider the distance of one feature is less than a specific fraction of the distance to the next nearest feature. In case of a false match, there will be a number of other near features with close distances, due to the dimensionality of the features.

On the other hand, in case of a correct match, it is unlikely to find another feature which is too close due to the highly distinctive nature of SIFT features.

LBP feature Extraction:-

Local binary Pattern (LBP) [18] is a feature extraction technique, mainly used for texture analysis. It is invariant to grey-scale transformations which are necessary for texture description. LBP method is suitable to explain texture and model of a digital image. This method can be done by splitting the images into number of small cells from which the features are extracted. The pixels in the small cells are described using binary patterns. The features that are formed from the cells are combined into a single feature histogram, which describes to model a representation of the image.

The LBP operator use decimal numbers to represents the pixels of an image, which are called LBPs or LBP codes. It encodes local structure around each pixel. Each pixel is compared with its eight neighbors in a 3 × 3 matrix by subtracting the center pixel value. If the result is less than zero, encode it with 0, otherwise with 1. In each pixel, a binary number is obtained by combining all these binary values in a clockwise direction starts from top-left neighbor. The corresponding decimal number of the resultant binary number is used for labeling the given pixel. This binary number is called LBPs or LBP codes. This can be illustrated in Fig.3. In large scale structures, LBP operators are unable to capture dominant features.



10	8	5
4	4	3
2	6	9

1	1	1
1		0
0	1	1

Binary: 11101101

Decimal: 237

Fig. 3:- LBP Method

Feature Selection:-

After extracting features from the scrambled images, then select important features for classification. This paper used a t-test for feature selection.

The t-test has been widely used to rank image features. For multiclass problem Tibshirani et al. [19] computed a t-statistics value for each image of each class by evaluating the difference between the mean of one class and the mean of all the other classes, where the within-class standard deviation is used for standardizing the difference.

$$t_{ic} = \bar{x}_{ic} - \bar{x}_{i/Mc. (Si + S0)} \qquad (3)$$

$$t_i = \max \{|\bar{x}_{ic} - \bar{x}_i| / M_c . S_i , c=1, 2,\ldots C\} \qquad (4)$$

Here t_{ic} is the t-statistics value for the i^{th} feature of the c^{th} class; $\bar{x}_{ic}$ is the mean of the i^{th} feature for the c^{th} class, and $\bar{x}_i$ is the mean of the i^{th} feature for all the classes. S_i is the within-class standard deviation and S_0 is the median value of S_i for all the features. The greater value of t-scores indicates that the feature is more relevant. This method uses 100 relevant features for classification.

Classification:-

After features are selected, classifications are performed using sparse classifier. After scrambling process, the features are randomly scattered in the feature space. So sparse classifier is suitable for randomly scattered distribution, it correctly classify the randomly distributed features.

Sparse representation based classifier:-

Sparse Representation based Classifier (SRC) can directly assign a label to a test image and it is a nonparametric learning method. SRC is a best combination of compressed sensing and machine learning. In SRC, the sample matrix is used as the sparse representation matrix and also uses some transformation matrix to reduce input space dimensionality. The training samples are represented in column of the matrix. Random projection (RP) is a good method for reducing dimensionality, since Wright et al. state that ”the precise choice of feature space is no longer critical, even random features contain enough information to recover the sparse representation and hence correctly classify any test image” [20].

Assume that there are a set of training samples $\{(x_i,y_i)\ (x_i \in X\ ),y_i \in \{1,2,\ldots..,c\},i=1,2,\ldots.,n\}$,where c is the number of classes, m is the dimensionality of the input space X. and y_i is label corresponding to x_i . Given a test sample $x\in X$, the goal is to predict exactly the label y of x from the given training class samples. Now we arrange the j^{th} class training samples as columns of a matrix $X_j=[x_{j,1},\ldots.,x_{j,nj}]$, $j=1,\ldots.,c$, where $x_{j,1}$ denotes the sample belonging to the j^{th} class, and n_j is the number of the j^{th} class training samples.

Define a new sample matrix for all training samples
$X=[X_1,X_2,\ldots,X_c]$. According to SRC, the test sample can be linearly represented by using all training samples:

$$x=X\alpha \qquad (5)$$

where α is the vector of coefficients. If the test sample x belongs to the j^{th} class, then the entries of α are expected to be zero except some of those associated with this class. $\alpha= [0,\ldots,0,\ \alpha_{j,1},\ldots..,\alpha_{j,nj},0,\ldots.,0]^T$ where $\alpha_{j,i}$ is the coefficient corresponding to the training sample $x_{j,i}$. Thus, the coefficient vector α is expected to be sparse. In SRC, the problem of finding the coefficient vector is formulated as a convex programming problem

$$\min||\alpha||_1 \text{ subject to } x=X\alpha \qquad (6)$$

where $||.||_1$ denotes the l_1-norm. Equation (4) is also called the l_1-minimization problem [21], [20]. Then compute the residual

$$r_i(x)=||x-X\alpha||_2 \text{ for } i=1,\ldots.c. \qquad (7)$$

$$\text{identity}(x)= \arg\min ri(x) \qquad (8)$$

Equation (8) gives the label of the test image.SRC shows very interesting robust Face Recognition (FR) performance.

Experimental Results:-

This section presents results obtained from the proposed system. In the experiment all code was implemented in MATLAB 2013 a, and ran on a PC with 2.40 GHz Intel-core CPU. In the experiment, use a test scheme called leave-k-out [22]. The experiments were carried out using ORL dataset [23] and Yale dataset [20]. The ORL dataset contains 40 subjects and each subject has 10 sample images. The Yale dataset contains 15 subjects and each subjects has 11 sample images. This dataset shows that the proposed system attains high rate of accuracy and reduce time consumption.

In leave- k- out test, if each subject has N faces in a dataset, we leave k faces for testing and remaining images are used for training purpose. So , the benchmark test will have (N-k) training faces per subject. Selecting k samples from N faces will have ${}_N^k$ choices. The accuracy is the average of all N tests. Here the k varies from 1 to 5. Fig.4 shows all leave-k-out tests.

Table I. lists the overall accuracy by averaging all k tests. Here, we compare ORL dataset and Yale dataset. The Yale dataset attains high accuracy around 96.3 %.

Table I:- accuracy of all k tests

Dataset	Accuracy
ORL dataset	96
Yale dataset	96.3

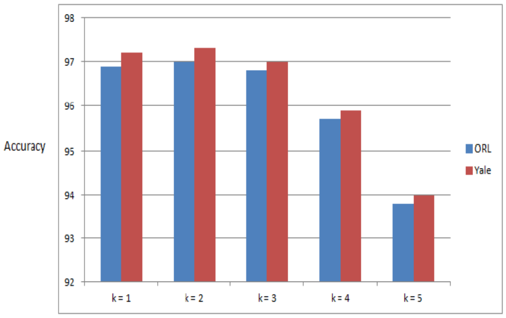


Fig. 4:- *Leave-k-out* tests.

Conclusion:-

A privacy protected facial verification system using sparse classifier in the scrambled domain is introduced. In the proposed method, the features are extracted from the scrambled face using SIFT and LBP feature extraction method and a t-test based feature selection method is used to select important features for classification. Then sparse representation based classifier is used for classifying the face images. Experiments shows that proposed face verification system attains high rate of accuracy and reduce time consumption. This method can be a promising candidate for emerging privacy-related facial biometric applications, especially for public visual surveillance systems where face scrambling is applied.

References:-

1. T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, T. Fujino, “Hierarchical image-scrambling method with scramble-level controllability for privacy protection,” Proc. IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), 2013, pp.1371-1374.
2. F. Dufaux, “Video scrambling for privacy protection in video surveillance: recent results and validation framework,” Proceedings of SPIE, Vol. 8063, 2011, pp.14.
3. A. Melle, J.-L. Dugelay, “Scrambling faces for privacy protection using background self similarities,” Proc. 2014 IEEE International Conference on Image Processing (ICIP), 2014, pp.6046-6050.
4. Y. Wang, T. Li, “Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System,” Proc. 2010 International Conference on Intelligent System Design & Engineering Application, 2010, pp.449-451.
5. Z. Tang, X. Zhang, “Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies,” Journal of Multimedia, Vol. 6, No. 2, April 2011, pp.202-206.
6. A. Erdlyi, T. Bart, P. Valet, T. Winkler, B. Rinner, “Adaptive Cartooning for Privacy Protection in Camera Networks”. Proc. International Conference on Advanced Video and Signal Based Surveillance, 2014, pp.6.
7. R. Jiang, A. H. Sadka, D. Crookes, “Multimodal biometric human recognition for perceptual human-computer interaction,” IEEE Trans. Syst. Man Cyber. - Part C Applications & Reviews, Vol.40, No.6, 2010, pp.676 -681.
8. Z. Ju, H. Liu, “A Unified Fuzzy Framework for Human-Hand Motion Recognition,” IEEE Trans. Fuzzy Systems, Vol. 19 , Issue 5, 2011, pp.901- 913
9. M. Rashid, S. A. R. Abu-Bakar, M. Mokji, “Human emotion recognition from videos using spatio-temporal and audio features,” The Visual Computer, Vol.29, Issue 12, Dec. 2013, pp.1269-1275.
10. R. Jiang, D. Crookes, N. Luo “Face recognition in global harmonic subspace,” IEEE Trans. Information Forensics & Security, Vol. 5, No. 3, 2010, pp.416-424.
11. A. Ghazanfar, D. Takahashi, “Facial Expressions and the Evolution of the Speech Rhythm,” J. Cognitive Neuroscience, June 2014, Vol. 26, No. 6, pp.1196-1207.
12. Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, “Privacy-Preserving Face Recognition,” Proc. Ninth Int’l Symp. Privacy Enhancing Technologies (PETS ’09), 2009, pp.235-253.
13. Eman A. Abdel-Ghaffar , Mahmoud E. Allam , Hala A. K. Mansour , and M. A. Abo-Alsoud, “A Secure Face Verification System Based on Robust Hashing and Cryptography,” 2009 IEEE., Issue 3, March 2015.
14. R.jiang,A.Bouridane, D.Crookes, M. Emre Celebi, Hua-Liang Wei,”Privacy Protected facial biometric verification via Fuzzy Forest learning,”proc. IEEE Transactions on Fuzzy Systems,2015, DOI 10.1109/TFUZZ.2015.2486803.

15. P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection," IEEE Trans. Pattern Analysis & Machine Intelligence, Vol. 19, No. 7, July 1997, 711-720.
16. Mohamed Aly,"Face recognition using SIFT features"
17. David G. Lowe. Distinctive image features from scale-invariant keypoints. International journal of computer vision, 60, 2004. Sarabjit Singh1**,**
18. Amritpal Kaur2, Taqdir," A Face Recognition Technique using Local Binary Pattern Method",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4
19. Tibshirani, R., et al. 2002. Diagnosis of multiple cancer types by shrunken centroids of gene expression.Proc. Natl. Acad. Sci. USA 99: 6567-6572.
20. J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 2, pp. 210–226, Feb. 2009.
21. A. Y. Yang, J. Wright, Y. Ma, and S. S. Sastry, Feature Selection in Face Recognition: A Sparse Representation Perspective EECS Dept., Univ. California, Berkeley, CA, 2007, Tech. Rep. Ucb/eecs-2007-99.
22. G. Cawley, N. Talbot, "Efficient Leave-One-Out Cross-Validation of Kernel Fisher Discriminant Classifiers," Pattern Recognition, Vol.36, No.11, 2003, pp.2585-2592.
23. F. Samaria, A. Harter, "Parameterisation of a Stochastic Model for Human Face Identification," Proc. 2nd IEEE Workshop on Applications of Computer Vision, Sarasota FL, December 1994.