International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

FUZZY FOREST LEARNING BASED ONLINE FACIAL BIOMETRIC VERIFICATION FOR PRIVACY PROTECTION

Supritha G M[1], Shivanand R D[2]

[1] *P.G. Student, Dept. of Computer Science and Engineering, B.I.E.T College, Karnataka, India*
[2]*Associate Professor, Dept. of Computer Science and Engineering, B.I.E.T College, Karnataka, India*

Abstract - *In public society, security plays a very important role everywhere. Video surveillance is one among those important fields. Privacy and security is important in the daily life of public society which is provided by the video surveillance. While distributing videos over public network there will be a chance of information loss but this should not happen in video surveillance as the facial images are the key information for those videos. To solve this issue Face scrambling method is used. In modern security technology the privacy under public surveillance can be maintained by scrambling the facial images. Thus as in scrambling domain the facial biometric verification has to be done. A biased random subspace scrambling is used for robustness in the scrambling process. And thus to maintain privacy and security in the video surveillance and for the images fuzzy forest learning scheme is applied. So the fuzzy decision trees are constructed and then the scrambled image can be found as the original image.*

Key Words: Fuzzy Forest Learning, Image Scrambling, LSDA, Fuzzy Decision Tree.

1. INTRODUCTION

In public society, security plays a very important role everywhere. Video surveillance is one among those important fields. Privacy and security is important in the daily life of public society which is provided by the video surveillance. In public and also in legal authorities privacy protection has become a major concern. While distributing videos over public network there will be a chance of information loss but this should not happen in video surveillance as the facial images are the key information for those videos. To solve this issue Face scrambling method is used. In modern security technology the privacy under public surveillance can be maintained by scrambling the facial images. Image scrambling has two advantages over encryption. The first advantage is Scrambling is supported for computing-efficient network targeted applications with the lower computation cost than the encryption. Scrambling can use the different parameters of Arnold Transform technique, where the scrambled faces are recovered by manual attempts in an easy way. But Decryption key is very important in encryption to get back the results. That is if a security guard wants to check the key face then he should have the decryption key to get that key face in surveillance video. Thus the purpose of public security control is less effective in encryption process.

Scrambling of an image can be done by using the following steps: (1) the image which is to be scrambled should create a matrix of the image which should be of the same size as the original image and then natural number is assigned to every element in that matrix. (2) The image matrix pixel coordinate with the generated matrix element value because the original image matrix is mapped by the generated matrix where it considers row by row and column by column for mapping. (3) Shifting the path by coordinating with the generated matrix is the key step. In this method every pixel is moved to the next position so if x is the coordinate then (x+1) mod s is the next coordinate position where the where the pixel is assigned. (4) In scrambling to make the image unrecognisable, the colour of the image and the position of the pixels are disarranged. To rebuild the original image some algorithms are found. (5)Scrambling can be done in two different ways: 2D matrix transformation and 2D Arnold transformation. Simplicity and periodicity are the main features of the Arnold Scrambling technology so that it is used widely in the image water marketing. After several cycles the restoring of an image can be done based on the periodicity of the Arnold Transform scrambling. The restoring of an image takes longer time as the periodicity depends on the size of the image in the Arnold scrambling.

Many methods have been introduced for the major issue of dimensionality reduction in the face recognition to achieve the challenge. Some of those methods are Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Fisher Linear Discriminant Analysis (FLD). These methods can also be used with the kernel methods by combining them. In 3D/2D face modeling techniques, by combining with many integrated with SVM algorithms and facial features, these approaches are applied.

1.1 System Design

In the pre-processing step, to scramble the image from the given training dataset, Arnold scrambling method is applied and these scrambled images are then forecasted towards the fuzzy forest learning process where many number of fuzzy decision trees are constructed from the randomly selected features. Then the forest decision process is utilized for the final decision where the fuzzy vector of membership is

created for each tree and forwarded for the further process. Then the Kullback-Lieder divergence method is used to get the final fuzzy decision from all the trees which depends on the fuzzy combination of all trees.

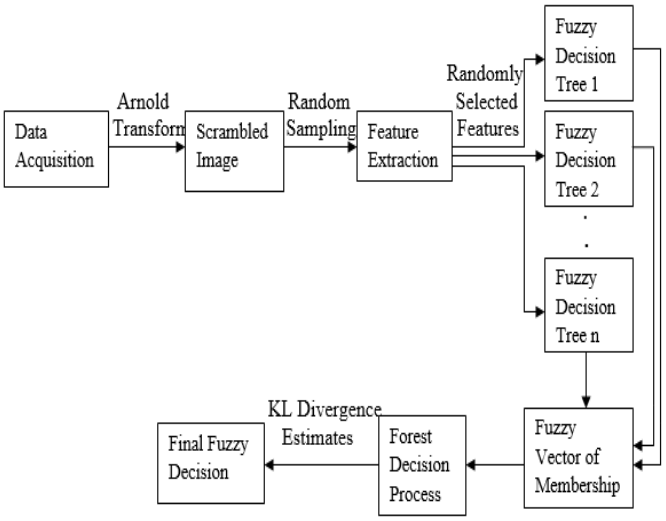

Fig -1: Schematic view of the Fuzzy Forest Learning

1.2 Methodology

1. Facial Biometric Verification in the Scrambled Domain

A. Face Scrambling utilizing the Arnold Transform Method

After transforming of the image, the image becomes chaotic and also meaningless pattern when digital image scrambling is applied. A process called information disguise is known for information hiding where it is treated like a pre-processing step which hides the image information. For information hiding, a non-password security algorithm is provided as the scrambling image technology and it is based on the data hiding technology. After the scrambling process the image becomes chaotic and therefore the public cannot see the visual contents of the image. Thus even if the image is distributed through the network the visual contents of the image cannot be accessed or browsed by the public or unauthorized user, as a result the privacy can be protected.

As the periodicity and simplicity are the two main properties of the Arnold scrambling algorithm, it can be a best method among the various image scrambling methods. Before applying this method to digital images it was called as cat-mapping. This method can easily be used as it has the property of simplicity. So this method is used for testing the scrambled face image domain. As in Arnold transform algorithm every pixel point is swapped to another point, it is known as two-dimensional Arnold scrambling.

After all the traversing of the pixel points a new image is produced by the Arnold Transform algorithm. So with the property of simplicity, cyclic and irreversible are also became the properties of the Arnold transform method. So even after the new image becomes chaotic the facial information of the original image will not be lost. Thus this method is more encouraged than the encryption as it cannot maintain the security needed for the facial images and the privacy is maintained by the Arnold Transform method by giving security for the images and prevents the exposing of facial information to the public.

2. Forest Learning Method Used For Scrambled Face Image.

A. Priori based Biased Subspace Sampling Method

The accuracy can be improved by using the multiple classifiers in the random forest reconstruction where being an aim of subspace sampling. From the available feature space from each pass in a random subspace feature selection, minimum numeral of dimensions are selected. In this method each classifier is dependent on the lower-dimensional subspace in a randomized selection. For the training data and test data, generalizing the classification of each tree is done from the selected set of features.

For constructing the forest small number of trees are considered rather than the larger number of trees. The high dimensionality features gives more option for the decisions practically than the other techniques which suffers from the scourge of dimensionality. As the complexity of the random forest increases the generalization of the accuracy increases as it take the advantage of the high dimensionality feature. Hence the random forest method is used to develop an advanced technique for constructing the high dimensional feature space. Henceforth, a complex methodology to develop any high-dimensional element spaces are normally supported in the company of random forest technique.

Human eyes gives more importance to the central features in the facial image like eyes, mouth regions etc. in face recognition method. Thus the central features are given more weight in the facial image as human can recognize the face. Hence for the central facial features, a biased randomization technique is used.

B. Construction of a Fuzzy Tree in a Random Forest

A fuzzy decision tree can be constructed using the selected feature subspace after selecting the features from each tree. The selected features space can be projected as eigenvector-based subspace by using the local sensitive discriminant analysis method for each tree. Thus to handle the face classification LSDA is used as an effective technique.

The dimension-reduced Eigen subspace is used for constructing the decision tree. In each subspace which is selected constructs the trees and then by using all the training data the trees are fully divided. Mutual information,

simulated annealing, clustering and many other splitting functions are used for constructing the trees. In each method there will be a variations and where in the subspace has unclassified points then a model is defined by a splitting function to project the classification with the training samples.

A simple linear split is used in constructing the fuzzy tree with the feature space translation. Then the anchor points chosen using the nearest-neighbour matching method by assigning the samples. After assigning, the anchor points which are closet to the class centroid are selected as the training samples. The training samples are same as leaves numbers in the tree which is having larger number of branches. In each node the query sample membership is computed in each tree for the fuzzy decision. Thus for every leaf node that is for training samples fuzzy membership is derived. And hence, the final output rather than the simple binary decision, the vector of memberships for all the leaves are created for a fuzzy tree.

3. Fuzzy Forest Decision

a. Weights of Fuzzy Tree Decision

Accuracy can be attained using the subspaces and the balance between the speed and accuracy can be obtained by the number of randomized trees and all the trees can be combined in some way where these are the challenges faced while using the features to build a forest. At each split, the construction of different trees can be done by selecting different feature dimensions. Thus the possibilities can be explored conveniently when the randomization is used during the dimension selection process.

An ensemble learning algorithm must contain mainly two aspects while constructing the random forest:

(i) To generate random trees selecting the proper subspaces or features is important.

(ii) In a rational and effective manner, the decision obtained from each tree are weighted and then a good combination of tree decisions are guaranteed.

(iii)

Through cross-validation in the forest the trees can be weighted using the proposed method and thus it is used for combining the decision trees for the face recognition in the random forest.

b. Fuzzy Forest Decision

In the process of fuzzy forest decision the neutralization of odd decisions are done where from each tree the estimation of the combination of weighted memberships are done and the fuzzy forest decision is based on this process.

The face images are scrambled from the given training dataset and those scrambled images are forecasted towards the fuzzy forest learning process. Then the weights are calculated from the central features where the features are selected randomly from the scrambled domain and from these selected features the fuzzy trees are constructed. Then for testing, scrambled face is given as input and then fuzzy vector of memberships are computed from each tree and it is forwarded to the forest decision process. Then the Kullback-Liebler divergence method is applied to weigh each tree from all the trees by the forest decision process and then by combining all the trees with the fuzzy process the final decision is derived.

2. Implementation Algorithms

2.1 Feature extraction from the face image:

Before scrambling, features are extracted from the face images like mouth, eyes and nose. Thus the algorithm for extracting the features from the face is given in the steps as:

Step 1: image_set, sets the image as global image
Step 2: Image path is given as the input using imagepath function
Step 3: imread reads the original image from the given path.
Step 4: BuildDetector detects the face and extracts the features from the face
Step 5: strcat concatenates the input image with the trained image in the training dataset
Step 6: imshow displays the feature extracted image.

2.2 Arnold Transform algorithm for image scrambling:

This Arnold transform algorithm is used for scrambling the face images. It takes only the square images for scrambling process so first step in this process is converting the images into square images. In this method the pixel points in the images are traversed or shifted from one point to another point and this is done for the matrix image as the row and columns are considered for the processing. That is the image is taken in Arnold Transform algorithm is N x N matrix format.

The algorithm for Arnold Transform scrambling is as follows:

Step 1: Input the Grayscale or RGB image I of the size MxN.
Step 2: Resize the image into N x N and convert it into grayscale image.
Step 3: Apply Arnold Transform to scramble the image.
Step 4: A pixel at the point (x, y) is swapped to another point (x^l, y^l). Where (x, y) = {0, 1, 2…N-1} That is (x, y) becomes $(x, y)^T$. Let p be the transform period of an N x N image.
Step 5: Repeat step 4 for k times. Where k=0, 1, 2 and so on. Which represents the number of iterations.
Step 6: Get the output as Scrambled image I^l.

2.3 Train procedure in Fuzzy Forest Learning:

Step 1: Scrambled train dataset is given as the input

Step 2: The dataset is then labelled
Step 3: F_{new} is a new feature space that is created using the weighting factor

Step 4: for k trees then n index numbers are generated
Step 5: Then the subsample F_{new} is obtained from n index
Step 6: LSDA is used to learn the discriminant features
Step 7: In the dimensionality reduction subspace, the tree is constructed.
Step 8: End loop.

2.4 Test procedure in in fuzzy forest learning:

Step 1: The forest constructed using the decision tree is given as input

Step 2: Scrambled image is given as a query image
Step 3: For k trees same subsamples are created for each tree
Step 4: Using LSDA eigenvectors the features are projected
Step 5: From all the classes the membership vector is calculated
Step 6: End loop
Step 7: Using fuzzy membership the weight of each tree is calculated
Step 8: The based on the fuzzy weights, all trees are combined
Step 9: Then display final fuzzy decision.

2.5 Fuzzy Forest decision tree:

The algorithm utilized to construct the decision trees and then finding the matched face for the input image given in steps as below:

Step 1: Require Test image and Eigen faces for input for recognition
Step 2: Projects the feature extracted image
Step 3: The input image is used as test image for testing
Step 4: imread reads the scrambled image as test image
Step 5: Euclidean distance is calculated for the image
Step 6: Minimum features are classified for the image
Step 7: The tree is constructed from the classified features
Step 8: The minimum features extracted and indexed and then sorted
Step 9: strcat is used to compare the images and the image is recognized
Step 10: imshow displays the matched image

3. Experimental Results

The face image of a person is given as an input for the scrambling of an image. In this the first step is, it selects the central features of the face like eyes, nose, mouth and then the whole face is selected for feature classification.

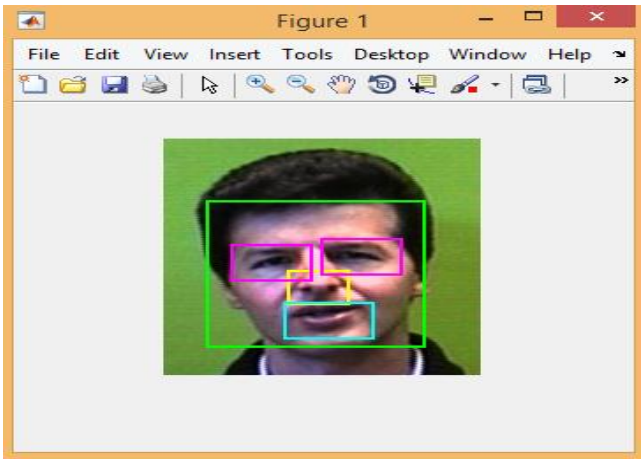

Fig-1: Input Image with the selected features

The given input image is then scrambled by using Arnold Transform Technique which is having the properties of simplicity and periodicity. All pixels of the original image are traversed from one point to another point and then the scrambled image is obtained for the original face image.

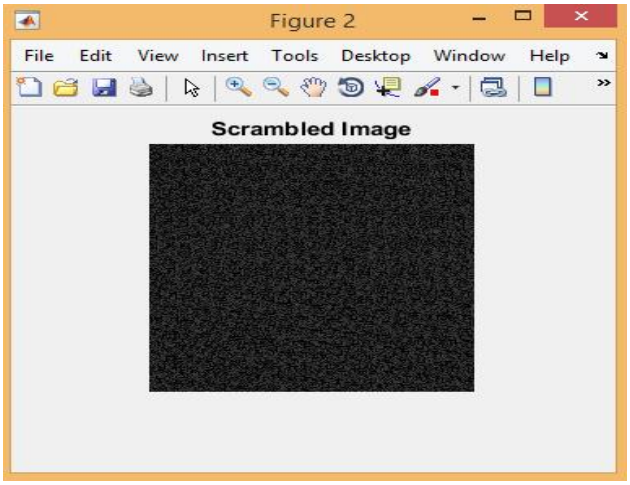

Fig-2: Scrambled Image

The test image is the scrambled image which uses the fuzzy forest learning scheme to randomly selecting the features from the scrambling domain for the feature classification of the images and then the selected features are used to construct a number of fuzzy trees. This scrambled image is given as an input for the test, where the fuzzy vector of membership is computed by each tree. The fuzzy vector of membership is then forwarded to the forest decision process where this process then weighs each tree with all other trees. Then the final decision obtained is dependent on the combination of all the fuzzy trees. The scrambled image which is given as the input test image as in the below figure.

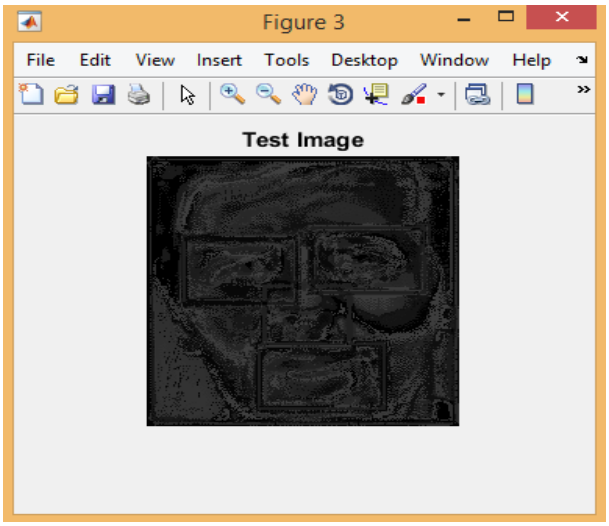

Fig-3: The scrambled image as input test image

After the complete process of fuzzy forest learning the scrambled image tested to match the original face image of a person. If the scrambled image is tested correctly with original image then it gives the result as matched image by giving the equivalent image same as the original image.

Fig-4: Matched image same as the original image

In the facial biometric verification the face image should match the original image of the person after all the process of scrambling. The face image of the person can be in any angle that is face can be in any angle or in any direction, the expressions of the person can be different at every stage but in biometric verification the person's image should match for every image where the expressions are different. When the original image matched with the face images of different angle then the result is displayed as matched face image of that person.

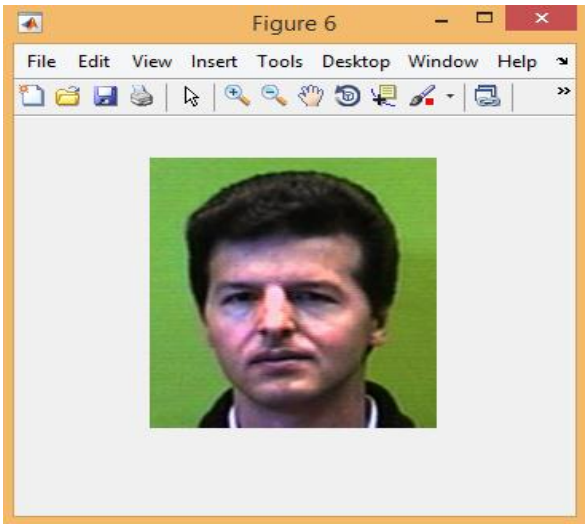

Fig-5: Different angled matched face image with the original image

Then it shows how the scrambling is done with the feature classification and how the decision tree is constructed to match the image. In this the image is classified to randomly select the features from the original face image where the image is classified by using a matrix form of rows and columns. All the pixels traversed from one point to another through these rows and columns. Then the features are classified where the minimum features which are nearer to the features of the other face images are identified and tested to get the decision trees. And then all the fuzzy trees compared with each tree which matches those selected features with its equivalent image and gives the result as a matched image. If the trained dataset contains many different images of the same person then the original image matches with all of the images and it displays the images that are matched as 'matched face image is:1.jpg, 2.jpg'.

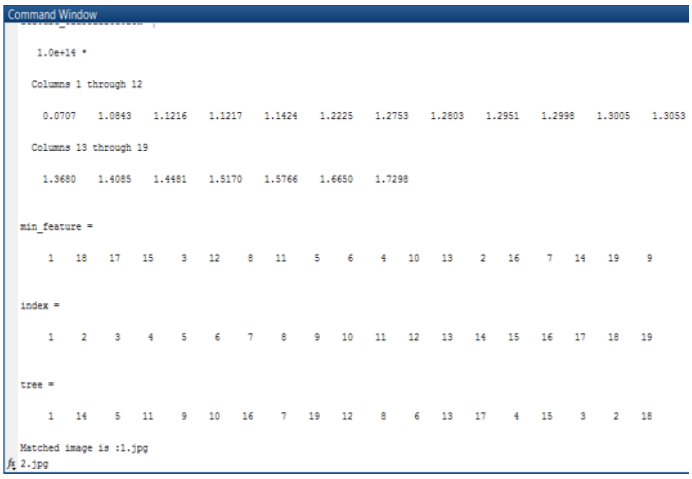

Fig-6: Result with the constructed decision tree

4. CONCLUSIONS

In the scrambled facial domain, a robust fuzzy forest learning procedure for facial biometric verification demonstrates how the fuzzy forest learning process can robustly cope with the instigation of tests in the scrambled face domain. Here the features that are extracted from the scrambled face images with the usage of random subspace sampling and then fuzzy decision trees are constructed from those selected features which are random. Hence the final fuzzy forest decision is acquired by utilizing the fuzzy decision membership vectors which are combined and weighted with all the fuzzy trees.

As this fuzzy forest learning process is vigorous to the challenging tests in the scrambled facial domain, the best accuracy is obtained consistently for the dataset which supports privacy related facial biometric applications. And the face scrambling is applied mainly in public visual surveillance systems where the privacy and security are the important aspects.

Fuzzy forest learning scheme is independent of any semantic 3D templates or face models. Semantic/3D face modelling is mainly targeted by the specific face features which can enhance accuracy but it may need computation time in extra and also it may cause extra errors. Thus the fuzzy forest learning process is used instead for the chaotic pattern classification cases like texture classification in analyzing the images or factor analysis of stock prices as it is purely based on the data-driven classification.

Thus in future work this fuzzy forest learning scheme can be applied in various applications to investigate the utilization of this methodology in the applications such as texture classification in analyzing the images or the factor analysis of stock prices.

REFERENCES

[1] 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.

[2] 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.

[3] Sohn Hosik, W. De Neve, Yong Man Ro, "Privacy Protection in Video Surveillance Systems: Analysis of Subband-Adaptive Scrambling in JPEG XR," IEEE Trans. Circuits and Systems for Video Technology, Vol.21, Issue 2, 2011, pp.170-177.

[4] F. Dufaux, T. Ebrahimi, "Scrambling for Video Surveillance with Privacy," Proc. 2006 Conference on Computer Vision and Pattern Recognition Workshop, Washington, DC, USA, 2006, pp.106-110.

[5] F. Dufaux, "Video scrambling for privacy protection in video surveillance: recent results and validation framework," Proceedings of SPIE, Vol. 8063, 2011, pp.14.

[6] T. Winkler, B. Rinner, "Security and Privacy Protection in Visual Sensor Networks: A Survey," ACM Computing Surveys, Vol.47, Issue 42, 2014, pp.1.

[7] 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.

[8] 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.

[9] 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.