ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

Facial Biometric Verification with Privacy Protection Using Fuzzy System

S.J.Grace Shoba[1], Akshaya.M[2], Kameswari.S[2], Sornalakshmi.G[2], Sivagami.S[2]

Professor, Dept. of ECE, Velammal Engineering College, Chennai, TamilNadu, India[1]

UG Student, Dept. of ECE, Velammal Engineering College, Chennai, TamilNadu, India[2]

ABSTRACT: Privacy plays a vital role in public security. Especially, while distributing videos over public network image privacy may become a major challenge. The image may be protected using some encryption methods, but this may sometimes lead to loss of image. This should not happen in video surveillance as the facial images are the key information for those videos. This issue can be solved by using scrambling method. The privacy can be maintained in modern security technology using image scrambling. When scrambling of images is done then facial biometric verification has to be done in scrambling domain which ensures image security. Arnold transform method can be used for scrambling of image. During a facial biometric verification, when image of a person is captured it is compared with scrambled image dataset. This comparison is done using the fuzzy forest system which creates number of decision trees. From the outputs obtained from the fuzzy trees the final decision is made. Once fuzzy decides the image, the particular image in the scrambled form can be recovered back to original form. This is performed using the Inverse Arnold transform and the original image is obtained from scrambled dataset.

KEYWORDS: Arnold transform, Fuzzy system, Decision trees, Inverse Arnold transform.

I.INTRODUCTION

In today's world, security and privacy plays a vital role. Especially private contents are going to be streamed. For example, consider a video surveillance clip that is going to be streamed over internet in such a case protecting the private content i.e., facial images is very important. Sometimes, distributing those videos over public network can cause loss of information but in case of video surveillance facial images are the prior information. Hence, the challenge is information must not be lost as well as its privacy must be protected. The images can be encrypted using some cryptographic key. But once if the key is lost it will lead to ultimate loss of image. Hence, it is not is the suitable method for privacy protection. In today's technology, scrambling the image can be the suitable method for protecting the privacy. Scrambling of image has several advantages over other privacy protection methods. Scrambling of image has low computational cost comparatively on network targeted applications. Hence, image scrambling serves to be effective public security method to image encryption.

In scrambling, the image which is to be scrambled should be in the same size as the original image and it should create a matrix of the image. Every element in the matrix is assigned with natural numbers. The original image is mapped with the generated matrix .here it considers row by row and column by column. In this method, coordinate is shifted to next position. For example if X is the coordinate that will be shifted to (X+1) position. The position of the pixels and color of the image are dislocated to make the image unrecognizable.

The process is repeated for desire number of cycles. Upon the completion of the entire number of cycles the restoring of image can be done based on the periodicity property of Arnold transform. The time taken for the restoration of image depends on size of the image. Due to the advantageous properties of Arnold transform method of scrambling it is also used for image water marking. Arnold transform method best suits for securing the image privacy rather than encryption since the restoration of image does not include the use of encryption key. In order to descramble the image in Arnold transform the parameter involved to dislocate the pixel points must be known. Hence the image privacy is maintained when a particular video is distributed over public network.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

The fuzzy forest method of learning is carried out in scrambled domain. This method involves the construction of N number of decision trees. The increase in number of decision trees will increase the complexity but improves the accuracy of the final decision. Although the fuzzy method of decision is robust it is reliable compared to other methods of making a reliable decision in scrambled domain.

II.LITERATURE SURVEY

Quist-aphetsi kester, mieee,"a cryptographic image encryption technique for facial-blurring of images" proposes an image encryption technique that will make it possible for selected facial area to be encrypted based on RGB pixel shuffling of an m*n size image. Cryptographic techniques for image encryption are normally based on the RGB pixel displacement where pixels of images are shuffled to obtain a cipher image. The pixel displacement and reshuffling of the image in steps between the processes has proven to be really effective. The extra transposition of RGB values in the image file after R G B component reshape has proven the increase of security of the image against all possible attacks [1].Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map" proposes only by means of XOR operation, a novel image encryption scheme is proposed based on a nonlinear chaotic map (NCM). There are two rounds in the proposed image encryption scheme. In each round of the scheme, the pixel gray values are modified from the first pixel to the last pixel firstly, and then the modified image is encrypted from the last pixel to the first pixel in the inverse order. In order to accelerate the encryption speed, every time NCM is iterated, n (n>3) bytes random numbers which are used to mask the plain-image can be gained. NCM is iterated, n (n>3) bytes random numbers can be gained so as to improve the encryption speed, and before next time iteration [2].Krishnan, G.S. Loganathan, "Color image cryptography scheme based on visual cryptograghy". Each pixel having 3 component as RGB. This RGB pixel value is first extracted and after shuffling we get the cipher image. It's done only by using the RGB value. Pixels having value are interchanged or displaced from their original position. The feature of the value is extracted and within the image [3].Zhenjun Tang and Xianquan Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies" proposes Arnold transform is a significant technique of image encryption, but has weaknesses in security and applications to images of any size. To solve these problems, the idea proposed is image encryption scheme using Arnold transform and random strategies. It is achieved by dividing the image into random overlapping square blocks, generating random iterative numbers and random encryption order, and scrambling pixels of each block using Arnold transform [4].Richard Jiang, Ahmed Bouridane, Danny Crookes, M.Emre Celebi, "Privacy-protected facial biometric verification using Fuzzy Forest Learning" proposes Arnold transform for encryption of the image, and uses the random forest method comparing the scrambled image database providing a high level of security. A biased random subspace sampling scheme is applied to construct fuzzy decision trees from randomly selected features, and fuzzy forest decision using fuzzy memberships is then obtained from combining all fuzzy tree decisions. In this experiment, we first estimated the optimal parameters for the construction of the random forest and, then, applied the optimized model to the benchmark tests using three publically available face datasets [5]. Melle and J.L.Dugelay, "Scrambling faces for privacy protection using background self-similarities" 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 [6]. Z. Erkin etal 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 image [7].Santhi,K.S.Ravichandran, A.P. Arun & L. Chakkarapani explains using images Features. Its uses Gray Level co-occurrence matrix of an image to extract the properties of an image [8].Ruisong Ye and Wei Zhou proposed a chaos based scheme for image encryption .In which chaotic orbits is constructed by using a 3d skew tent map with three control parameters. This generation is used to scramble the pixel positions .This approach having same good qualities such as sensitivity to initial control parameters pseudo-randomness [9].Extension to this approach for increasing the security purpose, Asia Mahdi Naser alzubaidi proposed a encryption technique using pixel shuffling with Henon chaotic. He divides scrambled image into sixty four blocks rotate each one in clockwise direction with go angle. For making distortion, two dimension Arnold Cat Mapping is applied and original position of pixel is reordered back to its original position [10].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

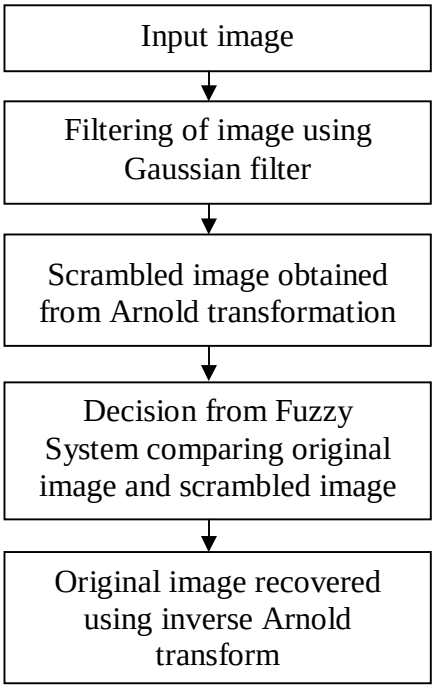
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

III.DESIGN OVERVIEW

Preprocessing step is especially for hiding the information of the digital image, which is also known as information disguise. In pre-processing Arnold transform method is used to scramble the image from the given dataset.



Then the scrambled images are forwarded to fuzzy forest learning process in which more number of fuzzy decision trees are constructed from the selected features. The decision of the forest is utilized for the final decision where the fuzzy vector membership is created for each tree. This is forwarded for further process. Then inverse Arnold transform is used to retrieve the original image from the scrambled one.

IV.TECHNIQUES IMPLEMENTED

A. FILTERING OF INPUT IMAGE

Public image datasets are used for this experimental purpose. The image dataset comprises of around 50 bitmap images of size 92*112 dimensions. The input image is filtered in order to remove the additional noise in image since it reduces the clarity of the image. For filtering of image Gaussian filter is applied. It removes the Additive White Gaussian Noise that are added during the transmission of image to the receiver. This filtering process before scrambling of image further improves the accuracy.

B. ARNOLD TRANSFORM FOR FACE SCRAMBLING

After applying the scrambling technique the image is changed into meaningless pattern of the image. This process is called information hiding that is original information is hide. 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 is done the image becomes chaotic and the public cannot know the original image. Even this streamed through public network the visual content cannot be track by the public and unauthorized users. As a result the privacy can be protected.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

Among the various image scrambling method Arnold scrambling algorithm suits to be the best due to its two major properties as periodicity and simplicity. Hence this method is used for testing the scrambled face image domain. Two dimensional Arnold scrambling methods involve every pixel point to be swapped another point.

Once every pixel points of the original image are swapped the completely new image is produced by Arnold transform algorithm. Arnold transform also possess the cyclic and irreversible properties.

In the Arnold transform, a pixel at the point (*x*, y) is shifted
To another point (*x*_, y_) as follows:

$$\begin{pmatrix} x1 \\ y1 \end{pmatrix} = 1 \begin{pmatrix} 1 & x \\ 1 & 2 \end{pmatrix} \begin{pmatrix} y \end{pmatrix}$$

which is called 2-D Arnold scrambling. The recursive and iterative application of the Arnold transform can be defined as follows:

$$P^{k+1}{}_{xy} = AP^{k}{}_{xy},\ P^{k}{}_{xy} = (x, y)^{T}$$

Here, the input is pixel (*x*, *y*)*T* after the *k*th Arnold transform, *Pk*+1xy on the left is the output for the (*k*+1)th Arnold transform.

Hence although scrambled chaotic images formed the original image will not get lost. Thus without using the encryption method privacy of the image is maintained by Arnold transform. The image is not lost as well as the image is not exposed.

V. IMPLEMENTATION OF FUZZY FOREST LEARNING METHOD

A. SUBSPACE SAMPLING METHOD

Improvement in the accuracy can be done by using multiple classifiers in the random forest. It is the main aim of subspace. From this features of spaces randomly subspaces are selected. Minimum numeral of dimensions is selected. In this technique each classifier depends on the lower dimensional subspaces in a randomized selection.

Initially small numbers of trees are built rather than large number of trees for constructing forest because increase number of features gives more option for decision as that complexity of the forest increases the accuracy increases. In subspace sampling method the major features are given more weight age in comparison to other features. The major features include regions like eyes mouth etc. These features are more important because the human beings can recognized them better.

B. FUZZY TREE CONSTRUCTION

A fuzzy decision tree can be constructed using the selected features subspace after selecting the features from each tree. The selected features space can be projected as eigenvector based subspace. The dimension reduced Eigen subspace used for constructing the decision tree. In each subspace which is selected constructs the trees and then by using all training data the trees fully divided.

The training samples are same as leaves numbers in the tree which is having larger number of branches. In each node the query members is computed in each tree for decision. Thus, the fuzzy training samples are derived. As the result, the final output rather than the simple binary decision, fuzzy tree are created from the vector membership.

VI. DECISION MAKING IN FUZZY FOREST

A. WEIGHTING METHODS IN FUZZY TREE

Through the fuzzy tree both the speed and accuracy must be attained. This can be attained by the increase number of random trees. The major challenge faced is combining this tress in some way to build the forest. At each spilt the selecting different feature dimension. In learning algorithm some of the aspects must be taken into account while constructing the random forest. On generating the random forest selecting the proper features is important.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

Decision are obtained from each tree are weighted. so that guaranteed tree decision can be obtained. Through cross validation of the trees effective decision can be obtained for the face recognition.

B. FUZZY FOREST DECISION

In the process of fuzzy forest decision the cancellation of odd decision were from each tree estimation of combination of weighted decision are done.

The face images are scramble from the dataset. Then the scrambled images are moved towards fuzzy forest learning process. The weights are calculated from major features where the major features are selected randomly from scrambled domain. When the fuzzy trees are constructed and the forest decisions are taken accordingly. Finally combining all the decision from the trees the final decision is made.

VI. DE-SCRAMBLING OF IMAGE USING INVERSE ARNOLD TRANSFORM

From the memberships constructed between the decisions trees in fuzzy system decisions are taken by the individual decision tree. The odd results are neglected and then the overall result is obtained by combining the results of all the individual decision tree results. The particular image is matched and the image in the scrambled form is recovered back to original form using the inverse Arnold transform algorithm. Inverse Arnold transform is the counter of Arnold transform. The particular parameter which is used to dislocate the pixel must be known in order to recover the original image back.

VIII.ALGORITHMS IMPLEMENTED

A.FACIAL FEATURE EXTRACTION

Input : Data set, set of images
Output: Feature extracted image
Process: Image path is given as input using image path function. imread reads the original image from the given path. Build detector detects the face and extracts features from space. imshow displays the feature extracted.

1. ARNOLD TRANSFORM ALGORITHM FOR IMAGE SCRAMBLING

Input : Grayscale or RGB image of the size
M X N
Output: Scrambled image
Process: Arnold transform is applied over the input image. The algorithm swaps the pixel at a point (x,y) to a new point (x1,y1). It takes P transform period for the entire image to be swapped. The same procedure is repeated for K number of times. Thus the scrambled image is obtained.

B.TRAINING PROCEDURE FOR FUZZY FOREST LEARNING

Input: Scrambled data set for training.
Output : Construction of forest from decision trees.
Process : A new feature space is built using centre biased map which is multiplied with a constant weighting factor. The following procedure is repeated for N trees.
Generation of N index numbers in random using the index number to subsample.
Construction of tree from subspace.

C. TEST PROCEDURE FOR FUZZY FOREST LEARNING

Input : forest constructed from decision tree and scrambled image.
Output: Fuzzy final memberships are formed from all classes.
Process: For the created 'K, number of Fuzzy trees similar subsamples are created. Then the features are projected using the Eigen vectors. Finally the membership vector is calculated and the final fuzzy decision is obtained.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

D. FUZZY DECISION TREE

Input : Test images for the matching purpose
Output: Displays the matched image
Process: The scrambled image is taken and the features are extracted at Eigen distances. The final decision after the fuzzy constructed image is compared with the matched image. imshow displays the matched image

XI.EXPERIMENTAL RESULTS

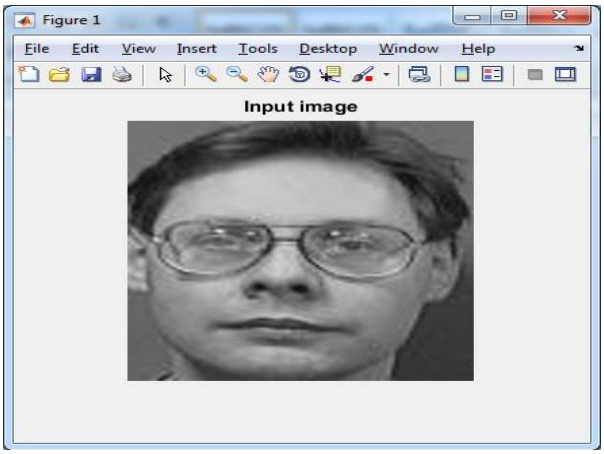


Fig-1: Original image

Fig-1 shows an image from the public dataset used for experimental purpose. The image before being given as input, it is preprocessed for better results. The noise from the image is filtered before undergoing the Arnold transformation.

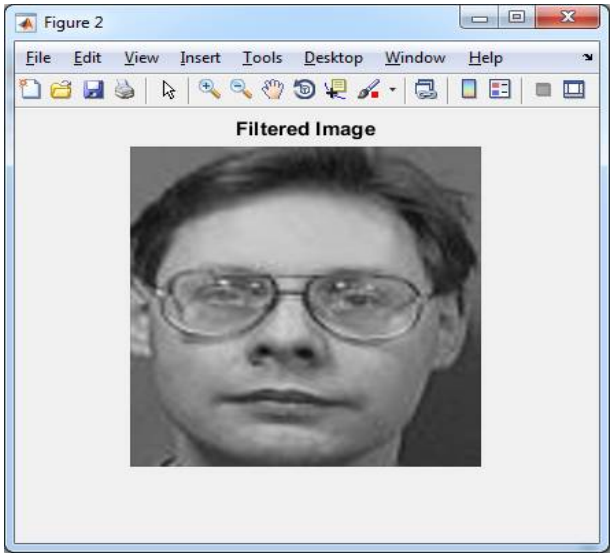


Fig-2 Filtered image of the original image

Removing the noise added to the image will give a better image after the scrambling and inverse scrambling process. Fig-2 shows the filtered image. The filtered image is given as input for
Arnold transforms.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

Arnold transform is applied to the given input image. The input image can be a Grayscale or RGB image. The coordinates of the original image are dislocated. That is the pixels are traversed from one point (x,y) to some new point (x1,y1). The process is carried for 'N' number of specified times. Then the scrambled image can be obtained. Fig-3 shows the scrambling of the filtered image using Arnold transform. The scrambled image is chaotic thus maintaining the privacy over the distribution of image.

Now when the image is to be matched fuzzy system is being used. Any further processing of the image must be carried out in the scrambled domain. Image remains secure and their will be no loss of data during the retrieval of the image as in other image hiding methods as masking, cartooning. The key factor involved in the image recovery is the constant using which the pixel points where multiplied to obtain a new location and the number of times this particular multiplication i.e. the number of shifts must be known in order to recover the image back.

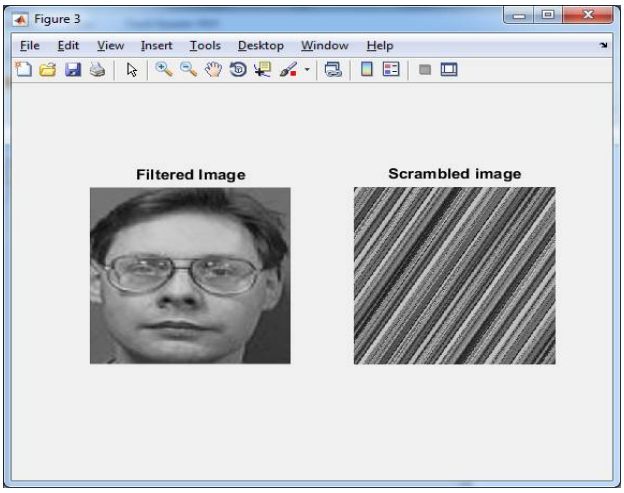


Fig-3 Scrambled image

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 various number of fuzzy trees. The scrambled image is given as an input for the test, where the fuzzy vector of membership is constructed by the decision trees.

Fig-4 Fuzzy constructed image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

The fuzzy vector of membership is then forwarded to the forest decision process where this process then weighs each tree comparing along with all other trees. The final decision is based on all the decision tree outputs. 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.

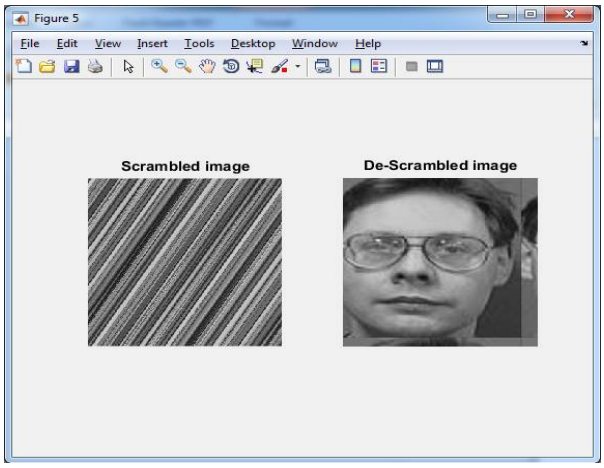


Fig-5 De-Scrambled image recovery

Consider the case where the image in the video of some surveillance camera must be revealed by some officials then the inverse Arnold transform is used to re-locate the traversed pixels back to its original position. This method of re-locating only requires the parameter of pixel shift 'N'. Fig-5 shows the de-Scrambling of the chaotic image back to the original form. De-scrambling using the inverse Arnold transform is simple since it only requires the constant with which the pixel location was multiplied to obtain a new location.

After the inverse Arnold transform the original image is displayed as the output. Thus the image privacy is maintained as the comparison is carried out in scrambled domain.

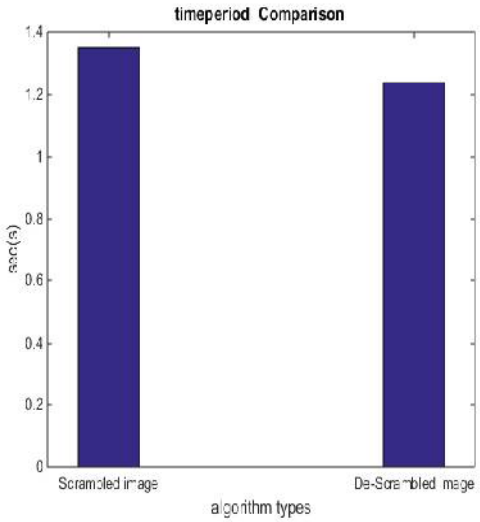


Fig-6 Timeperiod comparison between Arnold transformation and inverse Arnold transformation of image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

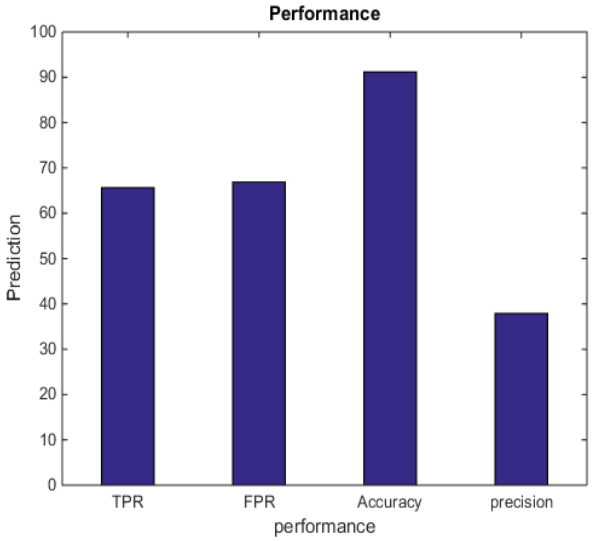


Fig-7 Performance result

The above figures show the comparison of the time taken by the Arnold transform to scramble the original image and the time taken by the inverse Arnold transform to de-scramble the image to original form Fig-6 and the values of the true positive rate, false positive rate, accuracy and precision Fig-7 respectively.

X.CONCLUSION

In this paper, a successful robust Fuzzy Forest Learning scheme for facial biometric verification in the scrambled domain is developed. In this scheme, to extract the features from scrambled face images robust, a biased random subspace sampling scheme is applied to construct fuzzy decision trees from randomly chosen features. Then, a fuzzy forest decision is obtained from all fuzzy trees features by the weighted combination of their fuzzy decision vectors of membership.

From the final decision taken by combining the resulting values of the individual fuzzy decision trees a particular image that matches the original image is chosen. Later, the particular image is descrambled by applying the inverse Arnold transform method. On comparing with the Arnold transform, inverse Arnold transform consumes more time. This system results True Positive rate value of 65.62 and False Positive rate value of 66.87. Applying Gaussian filter to the original image before scrambling improves the accuracy by 0.12 and the overall accuracy is 81.12 and the image precision 37.90.

It is worth highlighting that this approach is not dependent on 3-D face modelling can enhance accuracy, face modelling from images and facial component detection requires extra computation time and can also easily introduce additional errors. Instead, this approach is based purely on data-driven classification and can easily be applicable to other similar chaotic pattern classification cases, such as texture classification in image analysis or factor analysis of stock prices.

REFERENCES

1. Quist-aphetsi kester, mieee," a cryptographic image encryption technique for facial-blurring of images" in International Journal of Advanced Technology & Engineering Research (IJATER)
2. Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68, 2010
3. Krishnan, G.S.; Loganathan, D.; , "Color image cryptography scheme based on visual cryptography," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on , vol., no., pp.404
4. Zhenjun Tang and Xianquan Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies" Journal of multimedia , vol. 6, No. 2, April 2011

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

5. Richard Jiang, Ahmed Bouridane, Danny Crookes, M.Emre Celebi,"Privacy-protected facial biometric verification using Fuzzy Forest Learning", at IEEE transactions on fuzzy system,
vol.24, No.4 August 2016
6. A. Melle and J.-L. Dugelay, "Scrambling faces for privacy protection using background self-similarities," in Proc. IEEE Int. Conf. Image Process., 2014, pp. 6046-6050.
7. Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Proc. 9th Int. Symp. Privacy Enhancing Technol., 2009, pp. 235-253.
8. T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, and T. Fujino, "Hierarchical image-scrambling method with scramble-level controllability for privacy protection," in Proc. IEEE 56th Int. Midwest Symp. Circuits Syst., 2013, pp. 1371-1374.
9. S. Hosik, W. De Neve, and Y. M. Ro, "Privacy protection in video surveillance systems: Analysis of subband-adaptive scrambling in JPEG XR," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 2, pp. 170-177, Feb. 2011.
10. F. Dufaux and T. Ebrahimi, "Scrambling for video surveillance with privacy," in Proc. Conf. Comput. Vision Pattern Recog. Workshop, Washington, DC, USA, 2006, pp. 106-110.
11. M. L. Gao, L. L. Li, X. M. Sun, and D. S. Luo, "Face tracking based on differential harmony search," IET Comput. Vision, p.12,Jun,2014.
12. R. Jiang, D. Crookers, and N. Luo "Face recognition in global harmonic subspace," IEEE Trans. Inf. Forensics Security,vol.5,no.3,pp.416-424,sep.2010.