ISSN 2395-1621

Fuzzy Protected Privacy Based Face Recognition For Security system

[#1]Miss.Prachi Vetal, [#2]Prof. R.S.Pawase

[1]prachivetal07@gmail.com

[#1]PG Student, Department Of E&TC Microwave Engineering,
[#2]Assistant Professor, Department of E&TC

AVCOE Sangamner,
Savitribai Phule Pun University, Maharashtra, India.

ABSTRACT

The personal facial images should not be browsed without permission. online facial biometric verification needs to be carried out in the scrambled domain, thus a new challenge to face classification. In this paper, we investigate face verification issues in the scrambled domain and propose a novel scheme to handle this challenge.In this paper propose to make feature extraction from scrambled face images robust, 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 our 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. The experimental results validated that our proposed scheme can robustly cope with the challenging tests in the scrambled domain and achieved an improved accuracy over all tests, making our method a promising candidate for the emerging privacy-related facial biometric applications.

ARTICLE INFO

Article History

Received: 17th April 2019

Received in revised form :

17th April 2019

Accepted: 19th April 2019

Published online :

20th April 2019

I. INTRODUCTION

Deployment of video surveillance systems in urban environments has been a rapidly growing trend in recent years Together with the widespread adoption of such systems, we are now assisting to an equal growth in the introduction of automatic processing tools which are capable of interpreting the surveillance footage and extract high-level information such as people trajectories and identities. While many promoters argue that the adoption of such tools will lead to benefits such as crime prevention and increasing sense of security within the communities, several privacy advocates are legitimately concerned about the lack of effort in protecting the rights of the individuals being observed and in preventing misuse by the monitoring personnel. Current video surveillance systems are non-discriminative, in the sense that they cannot limit the monitoring activity to those subjects or behaviors which effectively pose a threat to safety . Recent trends in the research community show growing interest in a new approach to video surveillance architecture design which aims to integrate user privacy needs from the beginning, prior to the deployment of such systems . A major challenge in the design of privacy protection for video surveillance is to identify the correct balance between intelligibility of the source, which should be sufficient to perform typical monitoring tasks, and privacy protection itself. Ideally, the perfect privacy filter removes any personal information which could lead a human or a machine back to the identification of a subject, while retaining enough visual information for the human operator or the automatic algorithms to function correctly. While many privacy protection filters have been proposed addressing the privacy-intelligibility trade-off, for certain applications the removed personal information must be retained and made available for latter use, for instance to the authority in charge of suspect identification. Following this requirement, a number of approaches have been proposed which employ encryption techniques Nevertheless, such methods have the drawback of corrupting large portions of the original image, making the intelligibility task practically impossible. Other approaches utilize reversible scrambling applied in the compression-specific domain of a particular video format therefore obtaining a better visual result, but they end up depending on the compression algorithm in use. Taking into account these requirements, we propose a novel scrambling algorithm for protecting privacy sensitive ROIs (Region Of Interests) in an image, which encodes the sensitive data in a parametric form, exploiting the visual information in the remaining part of the image, i.e. the background. The

encoded data is encrypted with a secret key, and fully or partially decrypted to obtain a protected version of the original image at variable levels of scrambling. The knowledge of the full key enables decryption to a quality level suitable for subject identification. Our approach can be applied to any type of image content, but in this work we primarily focus on scrambling of faces, likely to be the most privacy sensitive region. To demonstrate the validity of the proposed approach we adopt an objective evaluation framework, by studying stateof-the art face recognition algorithms performance on the scrambled face images. Furthermore, we evaluate the quality of the results by an objective similarity metric close to the Human Visual System.

II. LITERATURE SURVEY

The author A.Melle and J.-L. Dugelay propose, The pervasive adoption of video surveillance systems demands tools for protecting the privacy of the persons being monitored. Current solutions are either native or they lack of important characteristics, such as reversibility or visual quality preservation. In this paper, we propose a novel scrambling procedure for protecting privacy sensitive image regions, which encodes the sensitive data in a parametric form, exploiting the visual information in the remaining part of the image. The encoded data is encrypted with a secret key. Partial knowledge of encryption key gives a protected version of the original image at variable levels of scrambling, while the knowledge of the full key allows decryption to a quality level suitable for people identification. To evaluate the proposed approach, we apply our scrambling filter to the AT&T face recognition dataset and we measure the resulting quality with an objective metric[1]

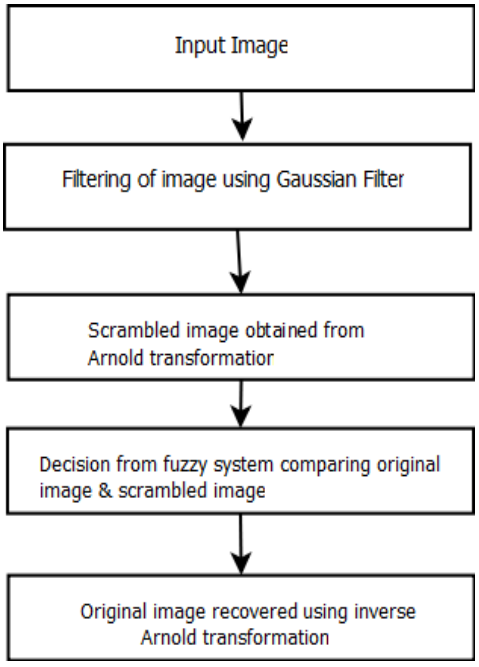
The author T.Winkler and B. Rinner, propose a Visual Sensor Networks devices come with image sensors, adequate processing power and memory. They use wireless communication interfaces to collaborate and jointly solve tasks such as tracking persons within the network. VSNs are expected to replace not only many traditional, closed-circuit surveillance systems but also to enable emerging applications in scenarios such as elderly care, home monitoring or entertainment. In all these applications, VSNs monitor a potentially large group of people and record sensitive image data which might contain identities of persons, their behavior, interaction patterns or personal preferences. These intimate details can be easily abused for example to derive personal profiles. The highly sensitive nature of images makes security and privacy in VSNs even more important than in most other sensor and data networks. However, the direct use of security techniques developed for related domains might be misleading due to the different requirements and design challenges[2]

The author S. Hosik,W. De Neve, and Y.M. Ro, propose a privacy-protected video surveillance system that makes use of JPEG extended range (JPEG XR). JPEG XR offers a low-complexity solution for the scalable coding of high-resolution images. To address privacy concerns, face regions are detected and scrambled in the transform domain, taking into account the quality and spatial scalability features of JPEG XR. Experiments were conducted to investigate the performance of our surveillance system, considering visual distortion, bit stream overhead, and security aspects. Our results demonstrate that subband-adaptive scrambling is able to conceal privacy-sensitive face regions with a feasible level of protection. In addition, our results show that subband-adaptive scrambling of face regions outperforms subband-adaptive scrambling of frames in terms of coding efficiency, except when low video bit rates are in use.[3]

The author Z. Tang and X. Zhang propose a Encryption is an efficient way to protect the contents of digital media. 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, we propose an 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. Experimental results show that the proposed encryption scheme is robust and secure. It has no size limitation, indicating the application to any size images[4]

III. SYSTEM ARCHITECTURE

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.



TECHNIQUES IMPLEMENTED

A. Filterring 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.

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.

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 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.

IV. ALGORITHAMS

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. I am reads the original image from the given path. Build detector detects the face and extracts features from space. I am show 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.

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

V. RESULTS AND DISCUSSION

Fig1: 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.

Fig2: Filter image to 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.
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.

Fig3: 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

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.

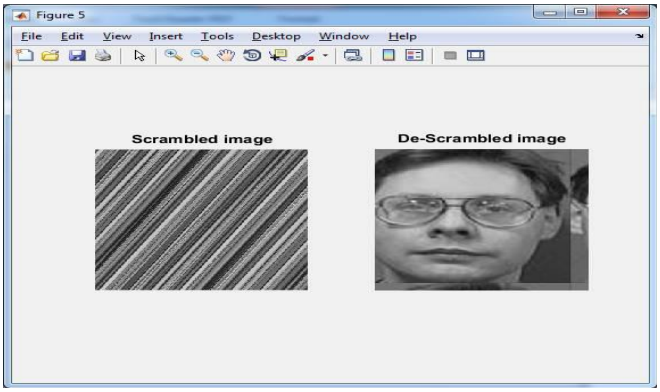
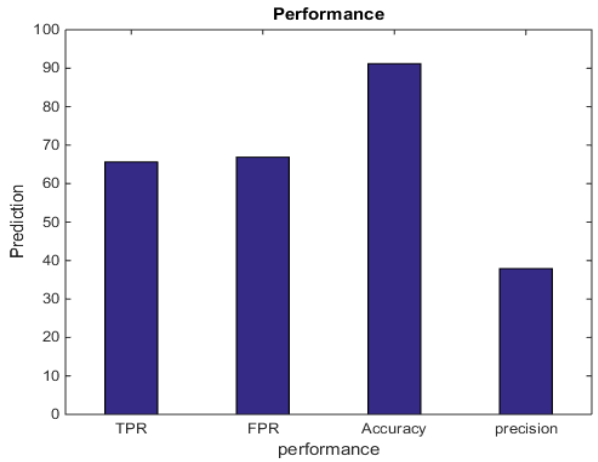


Fig-5 De-Scrambled image recovery

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.



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 and the values of the true positive rate, false positive rate, accuracy and precision respectively.

VI. 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.

REFERENCES

[1] 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.

[2]T.Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Comput. Surveys*, vol. 47, no. 1, p. 2, 2014.

[3]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.

[4]Z. Tang and X. Zhang, "Secure image encryption without size limitation using arnold transform and random strategies," *J. Multimedia*, vol. 6, no. 2, pp. 202–206, Apr. 2011.

[5] A. Erdlyi, T. Bart, P. Valet, T. Winkler, and B. Rinner, "Adaptive cartooning for privacy protection in camera networks,"in *Proc. Int. Conf. Adv. Video Signal Based Surveillance*, 2014, pp. 44–49.

[6]M. Rashid, S. A. R. Abu-Bakar, and M. Mokji, "Human emotion recognition from videos using spatio-temporal and audio features," *Visual Comput.*, vol. 29, no. 12, pp. 1269–1275, Dec. 2013.

[7] 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.

[8] R. Jiang, D. Crookes, and N. Luo "Face recognition in global harmonic subspace," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 416–424, Sep. 2010.

[9] H. Chang, Y. Yao, A. Koschan, B. Abidi, and M. Abidi, "Improving face recognition via narrowband spectral range selection using Jeffrey divergence," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 111–122, Mar. 2009.

[10]P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. fisherfaces:
Recognition using class specific linear projection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 711–720, Jul. 1997.

[11] M. H. Yang, "Kernel eigenfaces vs. kernel fisherface: Face recognition using kernel methods," in *Proc. Int. Conf. Autom. Face Gesture Recog.*,
2002, p. 215.

