International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

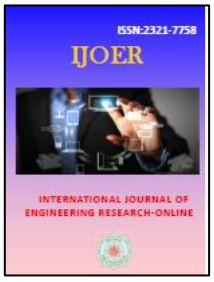
Vol.5., Issue.2, 2017
March-April

RESEARCH ARTICLE

ISSN: 2321-7758

SCRAMBLING FACE IMAGES FOR PRIVACY PROTECTION USING FUZZY FOREST LEARNING

ABIRAMI. P[1], VELLAISAMY. S[2], KALIMUTHU. T[3]
[1]PG Student, [2]Professor and [3]Assistant Professor
[1,2,3]Department of Electronics and Communication Engineering,
SCAD College of Engineering and Technology, Cheranmahadevi,TN, India.



ABSTRACT
Secure image communication is becoming increasingly important due to theft and manipulation of its content. Law enforcement agents may find it increasingly difficult to stay afloat above the ill intentions of hackers. To deal with this problem, facial image scrambling technique appears as a solution for privacy related applications. This project proposes scrambling face images for the purpose of privacy protection using fuzzy forest learning. The new technique involves in extracting datas from some special regions of the face and fed them to a fuzzy rule-based system. A Fuzzy classifier is applied to construct fuzzy decision trees from randomly selected features. A fuzzy membership is then obtained from combining all fuzzy tree decisions. Fuzzification operation uses membership functions. The distinct feature of a system is its simplicity and high accuracy. The experimental results validated that our proposed scheme can robustly cope with the challenging tests in the scrambled domain.
Keywords*:* Arnold transforms, fuzzy classifier, Fuzzification, face verification system.

1. INTRODUCTION

In the digital world, the internet is used for faster transmission of large volume of important and valuable data. Various confidential data such as government, military and banking and in other secured data, space and geographical images taken from the satellite and commercial important document are transmitted over the internet. Since internet has many points of attack; it is vulnerable to many kinds of attack, so this information needs to be protected from unauthorized access. To protect data from unauthorized access many data protection techniques are implemented. Digital image scrambling technology is an important way of securing digital image information.

With the use of transformation techniques, it can change the original image into a disordered one. Making it hard to recognize; for those who get the image in unauthorized manner to extract information of the original image from the scrambled images. The image after scrambling encryption algorithms is chaotic, so attacker cannot decipher it. By using multi-region scrambling, it can more effectively improve the security of image, lead decipher even more difficult.

2. RELATED WORKS

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.

R. Jiang et al. [7], proposes Face recognition in the Scrambled Domain via Salience-Aware Ensembles of Many Kernels. Here, a salience-aware face recognition scheme was used to work with chaotic patterns in the scrambled domain. In this

context, it becomes difficult to exploit landmarks or 3D models for better accuracy. Template-based face description has been considered to emphasize the importance of semantic facial components. The offline procedure then learns its semantic salience map. In the human perception system, concept-level semantic features are more meaningful than pixel level details. Scrambled facial recognition could generate a new problem in which many manifolds need to be discovered for discriminating these chaotic signals.

F.Dufaux and T.Ebrahami [1] address the problem of scrambling the regions of interest in a video sequence for the purpose of preserving privacy in video surveillance. They propose an efficient solution based on transform-domain scrambling. More specifically, the sign of selected transform coefficients is pseudo-randomly flipped during encoding. And they address more specifically the two cases of MPEG-4 and Motion JPEG 2000. Simulation results show that the technique can be successfully applied to conceal information in regions of interest in the scene while providing with a good level of security. Furthermore, the scrambling is flexible and allows adjusting the amount of distortion introduced.

S.Hosik, W De Nevve and Y.M.Ro [2] discuss privacy protected surveillance system by makes use of JPEG Extended Range (JPEG XR) and this JPEG XR is used to offer a low complexity solution for high resolution images. In this method the working was as follows. Initially face regions are detected and scrambled in the transform domain. The method was able to conceal privacy sensitive face regions with a feasible level of protection.

F. Dufaux [3] proposes a framework to assess the capacity of privacy protection solution of different face recognition algorithms. In order to assess the efficiency of algorithms they perform rigorous experiments with each of them. And in the paper they also introduce privacy protection techniques such as pixelization and blur.

T. Honda, Y. Murukami, Y. Yanagihara, T. Kumaki and T. Fujino [4] develop a paper which proposes an image scrambling method for bit map and JPEG XR formatted images. The method also enables access control by simply providing keys to authorized individuals. The major advantage with the method is that the image's format is retained and hence no special viewer is needed in display only console. And also the experimental results show that the scramble level can be linearly controlled by parameters. They also developed a demo system for describing the working and functionalities and to ensure that this can be implemented with embedded system such as those equipped with surveillance cameras.

A. Melle and J. L. Dugelay [5] propose a novel scrambling procedure for protecting privacy sensitive image regions which encodes the sensitive data in a parametric form, and exploiting the visual information in the remaining part. The data is encrypted with a secret key. Partial knowledge of the secret key reveals a protected version of the original image at variable level of scrambling and the knowledge of full key allows the decryption to a quality level suitable for people identification. To evaluate the proposed method they apply scrambling filter to the AT&T face recognition dataset and measure the resulting quality with an objective metric.

T. Winkler and B. Rinner [6] presents attacks that affect the data privacy in visual sensor networks and proposes privacy promoting security solutions based on opponent detection. In this paper considering the privacy and security mechanism for a heterogeneous wireless visual sensor network (VSN). The network consists of wirelessly communicating cameras and scalar sensors. The sensors trigger the cameras and provide specific privacy guarantees based on event detection. The network may deploy in one or more zones such as throughout a building and its perimeters.

3. METHODOLOGY

Digital images are increasingly sent over networks as documents, commercial items or law enforcement material. Due to the heightened activities of hackers all over the world, these images can easily end up in the hands of unscrupulous third parties who might profit/extort or modify them without the knowledge of the legitimate receiver. To safeguard the image information, research has been carried out in mathematics, cryptology and in information theory for the past two decade.

Previously, the image watermarking, the visual cryptology, the information sharing and the image scrambling has been proposed to counter image theft.

The objective of image scrambling is to generate a non-intelligible image which prevents human visual system or computer vision system from understanding the true content. It is easy only for an authorized user to descramble the image; the information regarding scrambling method and the variables are used in order to decipher the image.

This project presents a system that uses Arnold transform to encrypt an image. The number of times the transform is applied depends on a secret message expressed in a higher base. Arnold transform is an ergodic theory; it is also called cat mapping and then it is applied to digital image. Arnold scrambling algorithm has the feature of simplicity and periodicity. According to the periodicity of Arnold scrambling, the original image can be restored after several cycles. Digital images are scrambled and restored with the use of random upper (lower) triangular matrix and this method is of great application value due to its easy operation in encryption and decryption.

3.1 DESCRIPTION: The proposed FFL scheme used for the scrambled facial verification is as follows. Given a training dataset, faces are scrambled and forwarded to the FFL scheme. The procedure then randomly selects the features from the scrambled domain with biased weights toward central features, and a number of fuzzy trees are constructed based on the selected features, where LSDA is applied to further extract discriminant features from randomly selected features. After a scrambled face is input as a test, each tree computes a fuzzy vector of membership and forwards it to the forest decision process. The forest decision procedure then weighs each tree via their total Kullback–Lieder divergences from all other trees, while the final decision is based on a fuzzy combination of all trees.

3.2 INPUT IMAGE: The input image is taken as the behavioural sample. The images are collected from the Yale database [15]. This database contains fifteen persons and each person's has eleven sample faces. For the face verification this experiment uses the small dataset by splitting it into training and test dataset.

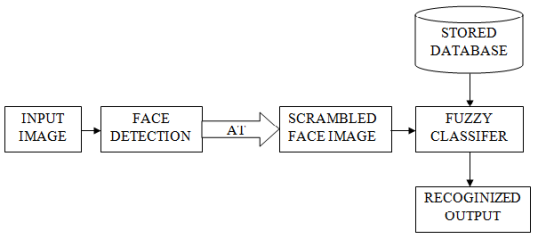


Figure.1 Block diagram of facial image scrambling method

3.3 FACE DETECTION: The function of this step is to determine whether the human face appear in the given image and check where the face is located. The human face has been selected from the input image and displays the patch in the input face image. This patch indicates that the face has been detected.

3.4 IMAGE SCRAMBLING: Scrambling is the pre-processing step. 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.

Figure 2 Scrambled face image

3.4.1 Arnold Transform: In the research of ergodic theory V.I Arnold proposed a method called Arnold transform. It has been called popular image scrambling method due to its simplicity and ease of

use. This method is used to provide security to the images.

In Arnold transform pixel position at (x, y) is transformed to another point (x', y') as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod N})\text{...Equation (1)}$$

Where (x, y) and (x', y') are the pixel coordinates of the original image and the encrypted image, respectively.

Let A denote the left matrix in the right part of Equation (1), I(x, y) and I(x', y') $^{(n)}$ represent pixels in the original image and the encrypted image obtained by performing Arnold transform n times, respectively.

Thus, image encryption using n times Arnold transforms can be written as:

$I(x', y')^{(k)} = AI(x, y)^{(K-1)} (\text{mod N})$ ....Equation (2)

Where $k = 1, 2, .., n$ and $I(x', y')^{(0)} = I(x, y)$.

3.5 FEATURE EXTACTION: Face image data has a very high dimensionality. To reduce the dimensionality data features are extracted from the scrambled face image.

3.6 FUZZY CLASSIFIER: The extracted features from the scrambled images, then select important features for classification. This project uses a t-test for feature extraction. After features are extracted, classifications are performed using classifier. After scrambling process, the features are randomly scattered in the feature space. So, kernel classifier is suitable for randomly scattered distribution, it correctly classifies the randomly distributed features.

3.6.1 Fuzzy Tree Construction: In the fuzzy tree construction, samples are assigned based on nearest-neighbour matching to chosen anchor points. The anchor points are selected as the training samples that are closest to the class centroids. These trees can have a large number of branches and can be very shallow. The number of leaves is the same as the number of training samples.

3.6.2 Fuzzy Forest Decision: The forest decision is usually based on a plurality vote among the classes decided by each tree. In this scheme, the vote from each tree is fuzzy, and the forest decision is based the combination of weighted memberships estimated from each tree, where odd decisions are neutralized in the fuzzy forest decision process The final decision is based on a fuzzy combination of all trees.

3.7 OUTPUT IMAGE: The two general applications of this face recognition method, the first is the identification and the second is the verification. Face identification helps to identify the face image by deciphering the scrambled image and also identifies ID Code of the authorized person based on the trained database.

4. 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. The Yale dataset shows that the proposed system attains high rate of accuracy and this method reduces the time consumption than other methods.

Table 1 Accuracy of various methods

Methods	PCA	KPCA	M-Kernel	Fuzzy
Accuracy	88.6	89.6	94.3	98.2

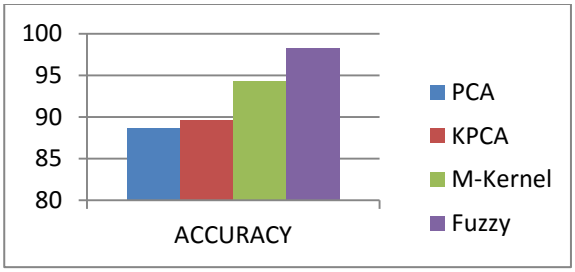


Figure 3 Accuracy graph

5. CONCLUSION

A privacy protected facial verification system using FFL in the scrambled domain is proposed. This method developed a robust FFL scheme for facial biometric verification in the scrambled domain. In the proposed scheme, to extract the features from scrambled face images and applied to construct fuzzy decision trees from randomly selected features. Then, a fuzzy forest decision is obtained from all fuzzy trees by the fuzzy classifier. It is worth highlighting that this approach is not dependent on any semantic face models.

Experiments shows that proposed face verification system attains high rate of accuracy and reduce time consumption. This method provides high security of images in the transmission process. Furthermore, by evaluation indicated that this method can flexibly control of scrambling with parameter sets regardless of contents in an image. Therefore, it can be applied to embed systems such as those equipped with surveillance cameras.

ACKNOWLEDGMENT

I am grateful to my project guide Professor Vellaisamy.S for his remarks, suggestions and also for providing all the vital facilities like providing the Internet access and important books, which were essential. I am also thankful to all the staff members of the Department.

REFERENCES

[1] F.Dufaux and T. Ebrahimi, (2006) "*Scrambling for video surveillance with privacy*," in Proc. Conf. Comput. Vision Pattern Recog. Workshop, Washington.

[2] S.Hosik, W.DeNeve, andY.M.Ro (2011) "*Privacy protection in video surveillance systems: Analysis of sub band-adaptive scrambling in JPEG XR*," IEEE TRANS. CIRCUITS SYST. VIDEO TECHNOL., VOL. 21, NO. 2.

[3] F. Dufaux (2011) "*Video scrambling for privacy protection in video surveillance: Recent results and validation framework*," PROC. SPIE, VOL. 8063.

[4] T. Honda, Y. Murakami, Y. Yanagihara, T.Kumaki, and T. Fujino (2013) *"Hierarchical image-scrambling method with scramble-level controllability for privacy protection*," in Proc. IEEE 56th Int. Midwest Symp. Circuits Syst.

[5] A.Melle and J.L.Dugelay (2014) *"Scrambling faces for privacy protection using background self-similarities*," in Proc. IEEE International. Conference for . Image Process.

[6] T.Winkler and B.Rinner (2014) "*Security and privacy protection in visual sensor networks: A survey*," ACM Computer Surveys, vol. 47.

[7] Jiang R., Maadeed S. A., Bouridane A., Crookes D., and Celebi M. E., (2016), "*Face recognition in the Scrambled Domain via Salience-Aware Ensembles of Many Kernels*," IEEE Trans. on Inform. Forensics and Security, vol. 11, no. 8, , pp. 1807-1817.

[8] Lin Y. Y., Liu T. L., and Fuh C. S., (2011), "*Multiple kernel learning for dimensionality reduction,*" IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 6, pp. 1147–1160.

[9] Wang D., Chang C., Liu Y, Song G., and Liu Y., (2015), "*Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values*" International Journal of Network Security, Vol.17, No.3, PP.322-327.

[10] Perakis .P, Passalis G., Theoharis T., and Kakadiaris I. A., (2013), "*3D facial landmark detection under large yaw and expression variations*," IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 7, pp. 1552–1564.

[11] Rahulamathavan Y., Phan R. C. W., Chambers J. A., and Parish D. J., (2013), "*Facial expression recognition in the encrypted domain based on local Fisher discriminant analysis*," IEEE Trans. Affective Comput., vol. 4, no. 1, pp. 83–92.

[12] Sim T., Baker S., and Bsat M., (2002), "*The CMU pose, illumination, and expression (PIE) database,*" in Proc. IEEE Int. Conf. Autom. Face Gesture Recognit., pp. 46–51.

[13] Taheri S., Patel V. M., and Chellappa R., (2013), "*Component-based recognition of faces and facial expressions*," IEEE Trans. Affective Comput., vol. 4, no. 4, pp. 360–371.

[14] Timotius I.K., Setyawan I., and Febrianto A., (2010), "*Face Recognition between Two Person using Kernel Principal Component Analysis and Support Vector Machines*", International Journal on Electrical Engineering and Informatics, Vol. 2, no. 1,pp-53-61.

[15] Yale database [Online]. Available: http://cvc.yale.edu.