ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/2886
DOI URL: http://dx.doi.org/10.21474/IJAR01/2886

RESEARCH ARTICLE

SCRAMBLING FACE IMAGES FOR PRIVACY PROTECTION USING ARNOLD TRANSFORM

Abirami. P
Department of Electronics and Communication Engineering, SCAD College of Engineering and Technology, Cheranmahadevi. India.

Manuscript Info

Manuscript History

Received: 21 November 2016
Final Accepted: 21 December 2016
Published: January 2017

Keywords:-
Scrambling face images, Arnold transform and kernel representation.

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 Arnold transform. In the proposed method, the facial features are extracted using Kernel Principle Component Analysis and the feature selection method is used to select important features for classification. This paper presents a system that uses Arnold transform to scramble an image. The number of times the transform is applied depends on a secret message expressed in a higher base. Then kernel representation based classifier is used for classifying the facial images. This kernel classifier transforms the scrambled image data into a three dimensions space through the mapping. The experiments show that the proposed face verification system identifies ID Code of the authorized person and solves the challenging tests in the scrambled domain.

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 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 techniques in digital images protection technique consist of two categories. One is watermarking and the other is encryption. The watermark-based techniques embed an invisible signal into the image to form a watermarked version. At the receiver's end, the integrity of image contents can be verified by authenticating the embedded signal. For encryption algorithms, produces an unintelligible or disorder image from the original image. Image encryption method is also called image scrambling. The image encryption algorithms are classified into two kinds. One is

Corresponding Author:- Abirami. P
Address:- Department of Electronics and Communication Engineering, SCAD College of Engineering and Technology, Cheranmahadevi. India.

spatial-based method; the other is frequency-based method. The spatial-based methods are usually achieved by swapping the pixel positions or altering pixel values. Arnold transform is widely applied to image encryption. The frequency based methods are exploited discrete prolate spheroidal sequences to design an image scrambling scheme without bandwidth expansion. However, the decrypted image is only equivalent to the original image.

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 the scrambled domain, semantic facial components simply become chaotic patterns. 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. Given a training dataset, faces are forwarded to the training procedure. 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.

T. Honda et al. [5], proposes the hierarchical image-scrambling method has three special features: restoration of the original image from only the scrambled image and its key, controlling of the scramble-level by using parameters for the length of random number and opening the image with a general image viewer. The image format structure is retained; therefore, it can be opened with a general image viewer. It can be used to protect privacy by scrambling images and the information of scramble area and parameter sets is included in the image. The images cannot view private information that they do not have permission to access. Experimental results suggest that scramble level can be controlled linearly by using parameters. The image format structure is retained. Therefore, it can be opened with a general image viewer. A scrambled image can be opened without a specific image viewer and retains the image format structure. The transforming process of an image is non-restorable; therefore the transformed information cannot be used as original information. It also increases the processing time.

A. Melle et al. [10], proposes a reversible scrambling technique which acts in pixel domain. The encoding parameters are encrypted using a secret key and then stored separately or alternatively embedded in the image itself by watermarking. The Region of Interest is decoded by parameters decryption with full or partial knowledge of the secret key, thus leading to different levels of scrambling alteration. This approach forms an objective quality perspective, showing that the visual quality decreases with increasing strength of scrambling. It obtains significant drop in recognition score and limiting the resolution of the encoding parameters. 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.

P. Perakis et al. [11], proposes a 3D landmark detection method for 3D facial scans. It based on Facial Landmark detector Model. The procedure involves landmark detection, labeling and selection. The detected and classified geometric candidate landmarks, from the shape index and the spin image maps are used as the candidate landmarks. These points create combinations of five landmarks, one from each class. The two types of landmark position constraints are used to reduce the search space (pruning) by removing obvious outliers and thus speed up the search algorithm. It offers high tolerance to large expression variations. It achieved by the state-of-the-art accuracy significantly out performing. The detection of a landmark with absolute distance error will work under certain threshold only. 3D landmark detection methods claim pose invariance, they fail to address large pose variations.

S. Taheri et al. [14]. proposes Component-based recognition of faces and facial expressions using a dictionary-based component separation algorithm. For this purpose, first generate two data-driven dictionaries, one for neutral components and the other one for the expression components. Knowing that the neutral component of the test face has sparse representation in the neutral dictionary and the expression part can be sparsely represented using the expression dictionary, then decompose the test face into these morphological components. The elements of the test face along with the dictionaries are then used for face and expression recognition. The algorithm finds a face model and facial expression that maximizes the likelihood of a given test image. The method for recognition of faces and expressions consider either the expression-invariant face recognition problem.

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 over the years. Previously, image watermarking, visual cryptology, information sharing and 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 very difficult for an authorized user to descramble the image using information regarding scrambling method and the variables are used in order to decipher the image.

This paper 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.

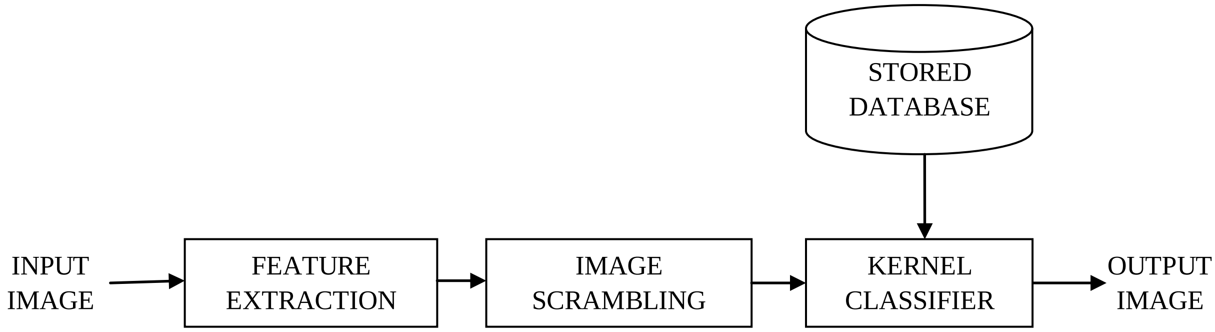


Figure.1:- Block diagram of facial image scrambling method

Description:-

The design three random strategies are used for scrambling the input image. These strategies improve the security and extend applications of Arnold transform.

They are as follows:-

- The first strategy is random division.
- The second is random iterative numbers.
- The third is random encryption order.

The proposed scheme is composed of three steps:-

- Face detection and feature selection.
- Image scrambling based on Arnold transform.
- Kernel mapping to extract the original image.

Input image:-

The input image is taken as the behavioral sample. The images are collected from the Yale database. 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 2:- Input image

Face detection:-

The main 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.

Image Scrambling:-

Scrambling is the preprocessing 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.

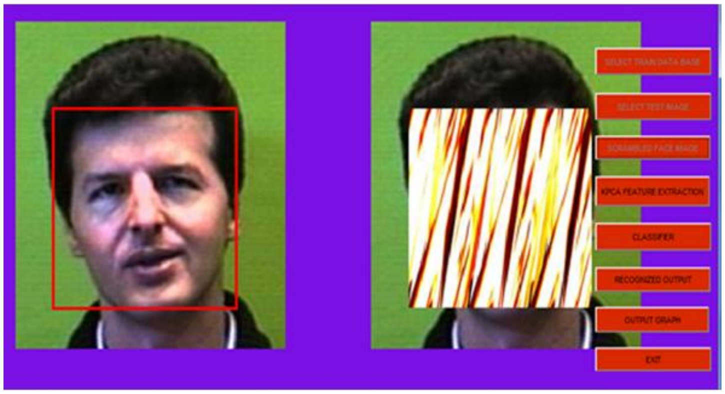


Figure 3:- Scrambled face image

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:

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

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:

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

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

Facial Feature Selection:-

The main facial regions are selected for the purpose of scrambling. The possible regions are detected by testing all the valley regions. Then all the possible face regions such as human eye, nostril and mouth corners are selected and perform scrambling. It is a widely used feature extraction technique which helps matching between same object of different views.

Kernel Principle Component Analysis (KPCA):-

KPCA is a development of the PCA (Eigen faces) method. PCA method is used in the feature extraction step of a face recognition system. Face image data has a very high dimensionality. To reduce the dimensionality data would contain only important features that we need in order to perform classification. PCA Performs very well in reducing the dimensionality of the data. However, the performance of PCA method (or other linear methods) is not completely satisfactory for problems with high nonlinearity, such as face recognition. Basically, the KPCA is used to tackle the nonlinearity of face recognition problem. By using a nonlinear kernel function, a dimensional reduction is performed.

Region Arnold Transform:-

Scrambling: Apply Arnold transform with the use of random upper (lower) triangular reversible matrix, and this method is of great application value due to its easy operation in encryption by N iterations. Then replace those original pixels with the scrambled pixels. Repeat the computation from i = 1 to i = K. The final result is the encrypted image. Therefore, digital images scrambled in this way become disordered in both pixel position

The security of our encryption scheme mainly depends on the random strategies. Since there are many possibilities of random division, attacker is very difficult to guess the division pattern. The used iterative number of Arnold transform when it is applied to the i-th regions. To improve security, this method produces a random order for processing these pixel regions.

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

Classifier:-

The extracted features from the scrambled images, then select important features for classification. This project uses a t-test for feature selection. After features are selected, 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.

Kernel Mapping:-

A kernel is a similarity function. Instead of defining a slew of features, a single kernel functions is used to compute similarity between images. The special characteristics of kernel classifier are it transforms the scrambled image data into a 3D space through the mapping. This embedding on a higher dimension is called the kernel trick or kernel mapping. The deciphering is performed by kernel mapping. After the N iteration steps of kernel mapping the original image retrieved. Thus, the kernel mapping obtains the original image from the scrambled image.

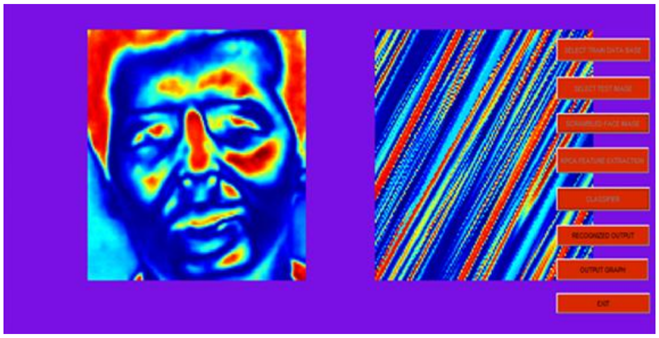
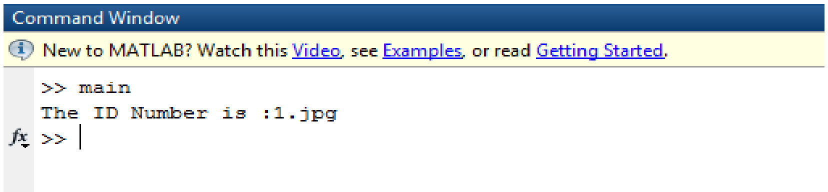


Figure 4:- Kernel map

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. The face verification is used to check whether the identified image is send by the authorized person and also identifies ID Code of the authorized person based on the trained database. Thus, the proposed method provides high secure and reliable.



New to MATLAB? Watch this Video, see Examples, or read Getting Started.

```
>> main
The ID Number is :1.jpg
>> |
```

Figure 5:- Authorized person ID Code output

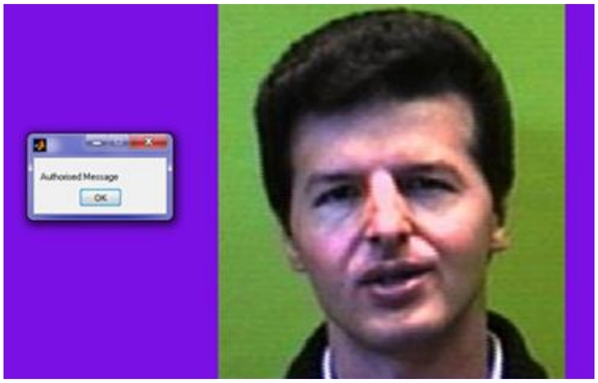


Figure 6:- Output image

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 contains 15 subjects and each subject has 11 sample images. This dataset shows that the proposed system attains high rate of accuracy and reduce time consumption.

Table 1:- Accuracy of various methods

METHOD	PCA	RDA	LDA	KLDA	LPP	KPCA
ACCURACY	76.0	76.0	80.0	81.5	83.1	91.5

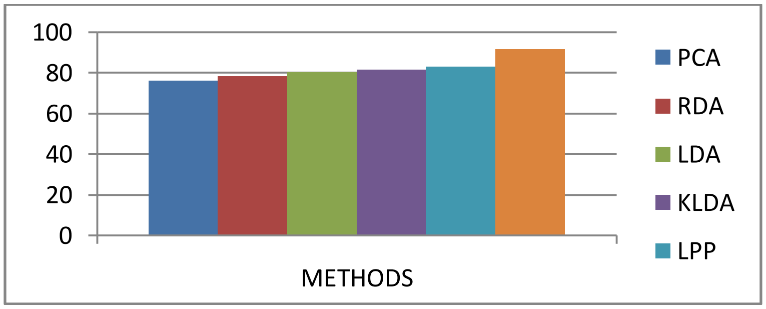


Figure 7:- Accuracy graph

Conclusion:-

A privacy protected facial verification system using kernel method in the scrambled domain is proposed. In this method, the features are extracted from the scrambled face using Kernel Principle Component Analysis feature extraction method and based feature selection method is used to select important features for classification. Through the Arnold transform, decomposition and recombination of pixels, the algorithm scrambles pixel positions and changes pixel values. Then kernel mapping based classifier is used for classifying the face images. During recombination, inflow of pixel values is avoided by conversion of number systems. Apart from disordering pixel positions and changing pixel values, this algorithm is able to diffuse errors.

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. The security of our scheme depends on the random strategies. Since there are many possibilities of random division, iterative numbers, and encryption order, attacker is difficult to correctly guess all random strategies at the same time. Thus, the security is guaranteed. Furthermore, our evaluation indicated that our method can flexibly control of scrambling with parameter sets regardless of contents in an image, There is little increase in processing time compared to non-scrambling when scrambling a face in an image; therefore, it can be applied to embedded systems such as those equipped with surveillance cameras.

References:-

1. Cootes T. F., Edwards G. J., and Taylor C. J., (2001), “Active appearance models,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685.
2. Draper B. A., Baek K., Bartlett M., and Beveridge J., (2003), “Recognizing faces with PCA and ICA,” Comput. Vis. Image Und., vol. 91, nos. 1–2, pp. 115–137.
3. Erdélyi A., Barát. T., Valet P., Winkler T., and Rinner B., (2014), “Adaptive Cartooning for Privacy Protection in Camera Networks,” in Proc. 11th IEEE Int. Conf. Adv. Video Signal Based Surveill., pp. 44–49.
4. He X., Yan S., Hu Y., Niyogi P., and Zhang H. J., (2005), “Face recognition using Laplacianfaces,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 3, pp. 328–340
5. Honda T., Murakami Y., Yanagihara Y., Kumaki T., and Fujino. T.,(2013), “Hierarchical image-scrambling method with scramble-level controllability for privacy protection,” in Proc. IEEE 56th Int. Midwest Symp. Circuits Syst. (MWSCAS), pp. 1371–1374.
6. Jiang R. and Crookes D., (2014), “Deep salience: Visual salience modeling via deep belief propagation,” in Proc. AAAI, Quebec City, QC, Canada, pp. 2773–2779.
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. McDuff D., Kaliouby R. E., and Picard R. W., (2012), “Crowdsourcing facial responses to online videos,” IEEE Trans. Affective Comput., vol. 3, no. 4, pp. 456–468.
10. Melle A. and Dugelay J. L., (2014), “Scrambling faces for privacy protection using background self-similarities,” in Proc. IEEE Int. Conf. Image Process. (ICIP), pp. 6046–6050.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. Wright J., Yang A. Y., Ganesh A., Sastry S. S, and Ma Y., (2009), “Robust face recognition via sparse representation,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 2, pp. 210–227.
18. Yale database [Online]. Available: http://cvc.yale.edu.