Face Image Recognition and Scrambling for Privacy using Neural Networks

S. Nithya
Assistant Professor, Dept. of ECE
K.Ramakrishnan College of Technology
Samayapuram, Trichy, Tamil Nadu, India.

S. Priyaa, R. Priyanka, S. Saranya
UG student, Dept. of ECE
K.Ramakrishnan College of Technology
Samayapuram, Trichy, Tamil Nadu, India.

***Abstract*— Privacy has become an issue of great concern in the transmission and distribution of surveillance videos. For example, personal facial image should not be browsed without authorization. Face image scrambling has emerged as a simple solution for privacy-related applications. Facial biometric verification needs to be carried out in the scrambled domain, thus bringing a new challenge to face classification. . In this paper, we explore face verification issues in the scrambled domain and propose a novel scheme to handle this challenge. In our proposed method, an efficient neural network is used in this system. Neural networks take a different move toward to problem solving than that of conventional computers. The experimental results validated that our proposed scheme can robustly cope with challenging tests in the scrambled domain and achieved an improved accuracy overall tests, making our method a promising candidate for the emerging facial biometric verification applications.**

Keywords—Arnold algorithm, Face Scrambling,Neural networs.

I. INTRODUCTION

An image is an artifact that depicts visual perception, for example a two-dimensional picture, that has a similar appearance to some subject usually a physical object or a person, thus providing a depiction of it. Image may be two dimensional, such as a photograph or screen display, or three-dimensional, such as a statue or hologram. They may be captured by optical devices such as cameras, mirrors, lenses, telescopes, microscopes, etc., and natural objects and phenomena, such as the human eye or water.

A volatile image is one that exists only for a short period of time. This may be a reflection of an object by a mirror, projection of a camera obscura, or a scene displayed on a cathode ray tube. A fixed image is one that has been recorded on a material object, such by photography or any other digital process

Binary images are also called bi-level or two-level. This means that each pixel is stored as a single bit—i.e., a 0 or 1. The names black-and-white, B&W, monochrome or monochromatic are often used for this concept, but may also designate any images that have only one sample per pixel, such as grayscale images. Binary images often arise in digital image processing as masks or as the result of certain operations such as segmentation, thresholding, and dithering.

In photography and computing, a grayscale or grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

Fig 1.1Color image Fig 1.2 Gray scale image Fig 1.3 Binary image

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

Digital image processing allows the use of much more complex algorithms, and hence, can offer both more sophisticated performance at simple tasks, and the implementation of methods which would be impossible by analog means.

In particular, digital image processing is the only practical technology for:

- Classification
- Feature extraction
- Multi-scale signal analysis
- Pattern recognition
- Projection

Due to the demands for greater public security over the past decade, video surveillance has become a widely applied technology in the day-to-day life of public

society. As a result, privacy protection has become a concern for the public as well as for the legal authorities. Key information such as facial images in surveillance videos should not be exposed when distributing videos over public networks.

II. EXISTING SYSTEM

To Make feature extraction from scrambled face images robust a biased random subspace sampling scheme is applied to construct fuzzy decision tree from randomly selected features and fuzzy forest decision using fuzzy membership is then obtained from combining all fuzzy tree decisions. 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, that scheme can robustly cope with the challenging tests in the scrambled domain and achieved an improved accuracy over all tests making the method a promising candidate for the emerging privacy related facial biometric applications. In comparison with encryption image scrambling has two apparent advantages.

First scrambling has much lower computation cost than encryption making it suitable for computing efficient network targeted applications. Second encryption may undermine the purpose of public security control because its check a key face in a surveillance video may not able to do so until him or her decryption key. In comparison scrambled faces using the Arnold transform can be easily recovered by manual attempts using the inverse Arnold transform with parameters.

There are many ways to perform face scrambling. For example scrambling can be done simply masking or cartooning. However this kind of scrambling will simply lose the facial information, hence face recognition becomes unsuccessful in this case. In addition for security it is obviously not a good choice to really erase human face from surveillance video. In contrast the Arnold transform as a step in many encryption algorithms is a kind of recoverable scrambling method. Scrambled faces can be scrambled by several manual tries. Because of this reason Arnold transform based scrambling as specific test platform. Automated surveillance systems are installed with online facial biometric verification. While it may not be permitted to unscramble detected faces without authorization due to privacy protection policies, the ability to carry out facial biometric verification in the scrambled domain becomes desirable for many emerging surveillance systems. Moreover unscrambling may involve parameters that are usually unknown by the online software the need arises to carry out face recognition purely in the scrambling domain. The task of automatically recognizing various facial images usually a challenging task. As a result face recognition has become a prominent research topic in image indexing, human computer, Sufficiently exploited for face recognition and to the best of our knowledge, very few reports on utilizing random forests for image based face recognition are publically available. An underlying reason is that a facial image cropped from videos usually has a small number of pixels such as (32 x 32), while random subspace sampling requires a larger number of features for sparse sampling.

Forest learning scheme to tackle the scrambled face recognition challenge. In the existing scheme a center surround prior map is applied to guide the random sampling in the scrambled domain, and a fuzzy decision making mechanism is introduced to weight tree decision via their fuzzy membership vectors. Then carried out an experimental validation on several scrambled face databases to show the effectiveness of proposed fuzzy scheme over scrambled facial images.

In the proposed system, face scrambling technique is used to protect the faces in the datasets. The faces in the datasets are scrambled used Arnold scrambling algorithm. Whenever the system needs access to the datasets, it will descramble the image and search for the match. The method used for scrambling is kept secretly.

The proposed system has some advantages such as the scrambling method is secret. Privacy is maintained even if the system is hacked. And also No one can add their identity without the admin authorization.

In this project we use the neural network method instead of Fuzzy forest learning. An Artificial Neural Network (ANN) is an information processing paradigm inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons. This is true of ANNs as well.

The Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. A trained neural network can be thought of as an “expert” in the category of information it has been given to analyze. This expert can then be used to provide projections given new situations of interest and answer “what if” questions.

A. Neural network Advantages:

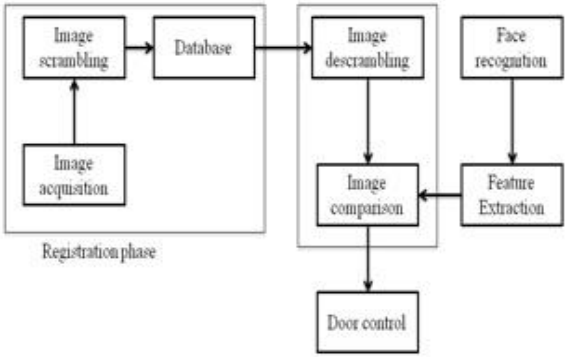
1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organization: An ANN can create its own organization or representation of the information it receives during learning time.
3. Real time operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.
4. Fault Tolerance via Redundant Information Coding: Partial destruction of a network leads to the corresponding degradation of performance. However,

some network capabilities may be retained even with major network damage.

B. Neural Network Application

1. Sales forecasting
2. Industrial process control
3. Customer search
4. Data validation
5. Risk management
6. Target marketing
7. Neural networks in medicine like Electronic noses, Instant physician, Modeling and Diagnosing the Cardiovascular system Units

C. Block Diagram



Data acquisition:

It is used in registration phase, this module perform the task of acquiring the authorized persons image and upload it into our algorithm.

Image scrambling:

It is used to protect the registered users face from the unauthorized persons. It performs scrambling by changing the location of feature points of the users face in a predefined manner. In this technique we use Arnold transformation to perform that task.

Classification database:

This classification database module holds the users scrambled image. This database will be maintained in the secure system in order to protect it from non authorized users.

Feature extraction:

Feature extraction starts from an initial set of measured data and builds derived values. When a person stood before the door, the camera will capture his/her image and calculate the feature points from the image.

Performance evaluation:

Thus the face scrambling technique performance which is used to protect the faces in the datasets has been evaluated. Whenever the accesses to the datasets are needed, it will descramble the image and search for the match. This technique is kept secretly.

Image comparison:

In the image comparison block the descrambled image from the database and feature points from the face compared for a much.

Door control:

This door control block open the door, if the image comparison block finds a match for the person in database. Otherwise, it will do nothing.

III. ARNOLD TRANSFORM ALGORITHM

A. Face Scrambling Using Arnold Transform

Digital images scrambling can turn an image into chaotic and meaningless pattern after transformation. It is a preprocessing step for hiding the information of the digital image, which is also known as information disguise. Image scrambling technology depends on data hiding technology, which provides non-password security algorithm for information hiding. The image after scrambling is chaotic and as a result the visual information is hidden from the public eye and privacy is then protected to a degree even if the visual contents are browsed or distributed over a public network.

IV. VARIOUS STEPS FOR DESIGNING A NEURAL NETWORKS MODELS

Step 1: Variable selection The input variables important for modeling/ forecasting variable(s) under study are selected by suitable variable selection procedures.

Step 2: Data Preprocessing

Data preprocessing refers to analyzing and transforming the input and output variables to minimize noise, highlight important relationships, detecting trends and flatten the distribution of the variables to assist the neural network in learning the relevant patterns. This also can be achieved by normalization. The choice of the normalization methods usually depends on the composition of the input vector. The following formulae are frequently used

Linear transformation to $[0,1]$: $\frac{x_0 - x_{\min}}{x_{\max} - x_{\min}}$

statistical normalization: $\frac{x_0 - \bar{x}}{s}$

simple normalization: $\frac{x_0}{x_{\max}}$

Step 3: Partitions of data sets viz. training, testing and validation sets The data set is divided into three distinct sets called training, testing and validation sets. The training set is the largest set and is used by neural network to learn patterns present in the data. The testing set is used to evaluate the generalization ability of a supposedly trained network. A final check on the performance of the trained network is made using validation set. Step 4: Neural networks paradigms Neural network architecture defines its structure including number of hidden layers, number of hidden nodes, activation function and number of output nodes etc.

(a) Number of hidden layers: The hidden layer(s) provide the network with its ability to generalize. In theory, a neural network with one hidden layer with a sufficient number of hidden neurons is capable of approximating any continuous function. In practice, neural network with one and occasionally two hidden layers are widely used and have to perform very well. (b) Number of hidden nodes:

There is no magic formula for selecting the optimum number of hidden neurons. However, some thumb rules are available for calculating number of hidden neurons. A rough approximation can be obtained by the geometric pyramid rule proposed by Masters (1993). For a three layer network with n input and m output neurons, the hidden layer would have sqrt(n*m) neurons.

(c) Number of output nodes: Neural networks with multiple outputs, especially if these outputs are widely spaced, will produce inferior results as compared to a network with a single output.

(d) Activation function: Activation functions are mathematical formulae that determine the output of a processing node. Most units in neural network transform their net inputs by using a scalar-to-scalar function called an activation function, yielding a value called the unit's activation. Except possibly for output units, the activation value is fed to one or more other units. Activation functions with a bounded range are often called „squashing functions". Appropriate differentiable function will be used as activation function. Some of the most commonly used activation functions are

(a) The sigmoid (logistic) function

$$f(x) = (1+\exp(-x))^{-1}$$

(b) The hyperbolic tangent (tanh) function

Step 5: Evaluation criteria The most common error function minimized in neural networks is the sum of squared errors. Other error functions offered by different software include least absolute deviations, least fourth powers, asymmetric least squares and percentage differences.

Step 6: Neural networks training Training a neural network to learn patterns in data involves iteratively presenting it with examples. The objective of training is to find the weights between the neurons that determine the global minimum of the error function. Multilayer feed forward neural network or multi layer perceptron (MLP), is very popular and is used more than other neural network type for a wide variety of tasks. Multilayer feed forward neural network learned by back propagation algorithm is based on supervised procedure, i.e., the network constructs a model based on examples of data with known output.

Step 7: Implementation The developed neural networks can be implemented for the unseen part of data or future data for prediction as well as classification.

V.EXPERIMENTAL RESULTS

Image acquisition:

The first stage of any vision system is the image acquisition stage. In this block, the image uploading will take place.

Fig:5.1. face image recognition.

In this process set of images are trained, the images are stored in the datasets.

Fig.5.2.a.input fig 5.2 b. scrambled image

A database is an organized collection of data. various scrambled images are stored in the database. Each images have a scrambled datasets, after the Arnold transformation. Neural networks are composed of simple elements operating in parallel. These elements are inspired by biological nervous systems. As in nature, the network function is determined largely by the connections between elements. We can train a neural network to perform a particular function by adjusting the values of the connections (weights) between elements.

Fig 5.3. Reconstructed training images

In the image comparison block the descrambled image from the database and feature points form the face are compared for a match.

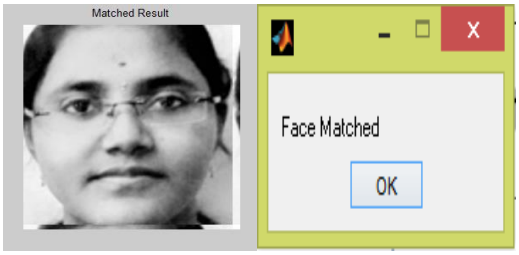


Fig 5.4. Face Matched Image.

In this door control block opens the door, if the image comparison block finds a match for the person in database. Otherwise, it will do nothing.

VI.CONCLUSION

We investigated face verification issues in the scrambled domain and proposed a novel scheme to handle this challenge. For that purpose an efficient neural network is used in this system. It is worth highlighting that our approach is not dependent on any semantic face models or 3-D templates. Although face specific features targeted toward semantic/3-D face modeling can enhance accuracy, face modeling from images and facial component detection needs extra computation time and can also easily introduce extra errors. Instead, our approach is based purely on data-driven classification and can easily be applied to other similar chaotic pattern classification cases, such as texture classification in image analysis or factor analysis of stock prices. In our future work, we plan to investigate the use of our method in these applications.

VII.FUTURE ENHANCEMENT

It is worth highlighting that our approach is not dependent on any semantic face models or 3-D templates. Although face specific features targeted toward semantic/3-D face modeling can enhance accuracy, face modeling from images and facial component detection needs extra computation time and can also easily introduce extra errors. Instead, our approach is based purely on data-driven classification and can easily be applied to other similar chaotic pattern classification cases, such as texture classification in image analysis or factor analysis of stock prices. In our future work, we plan to investigate the use of our method in these applications.

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] 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.
[3] 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.
[4] 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.
[5] 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.
[6] F. Dufaux, "Video scrambling for privacy protection in video surveillance: Recent results and validation framework," Proc. SPIE, vol. 8063, p. 806302, 2011.
[7] 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.
[8] 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.
[9] Y.Wang and T. Li, "Study on image encryption algorithm based on Arnold transformation and chaotic system,"in Proc. 2010 Int. Conf. Intell. Syst. Des. Eng. Appl., 2010, pp. 449–451.
[10] 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.
[11] R. Jiang, A. H. Sadka, and D. Crookes, "Multimodal biometric human recognition for perceptual human-computer interaction," IEEE Trans. Syst. Man Cybern. C, Appl. Rev., vol. 40, no. 6, pp. 676–681, Nov. 2010.
[12] Z. Ju and H. Liu, "A unified fuzzy framework for human-hand motion recognition," IEEE Trans. Fuzzy Syst., vol. 19, no. 5, pp. 901–913, Oct. 2011.
[13] D. J. Kim and Z. Bien, "Design of 'personalized' classifier using soft computing techniques for 'personalized' facial expression recognition," IEEE Trans. Fuzzy Syst., vol. 16, no. 4, pp. 874–885, Aug. 2008.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] A. Ghazanfar and D. Takahashi, "Facial expressions and the evolution of the speech rhythm," J. Cognitive Neurosci., vol. 26, no. 6, pp. 1196–1207, Jun. 2014.
[19] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cognitive Neurosci., vol. 3, no. 1, pp. 71–86, 1991.
[20] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the
gap to human-level performance in face verification," in Proc. IEEE Conf.
Comput. Vision Pattern Recog., 2014, pp. 1701–1708.
[21] B. Draper, K. Baek, M. Bartlett, and J. Beveridge, "Recognizing faces with PCA and ICA," Comput. Vision Image Understanding, vol. 91, nos. 1/2, pp. 115–137, 2003.
[22] 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.
[23] M. H. Yang, "Kernel eigenfaces vs. kernel fisherface: Face recognition using kernel methods," in Proc. Int. Conf. Autom. Face Gesture Recog., 2002, p. 215.
[24] T. F. Cootes, G. J. Edwards, and C. J. Taylor, "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, Jun. 2001.
[25] R. Hsu and A. Jain, "Semantic face matching," in Proc. IEEE Int. Conf. Multimedia Expo., 2002, pp. 145–148.
[26] O. Ibanez, O. Cordon, S. Damas, and J. Santamaria, "Modeling the skull–face overlay uncertainty using fuzzy sets," IEEE Trans. Fuzzy Systems, vol. 19, no. 5, pp. 946–959, Oct. 2011.
[27] S. Mian, M. Bennamoun, and R. Owens, "An efficient multimodal 2d-3d hybrid approach to automatic face

recognition," IEEE Trans. Pattern Anal.Mach. Intell., vol. 29, no. 11, pp. 1927–1943, Nov. 2007.

[28] Y. W. Pang, X. L. Li, Y. Yuan, D. C. Tao, and J. Pan, "Fast haar transform based feature extraction for face representation and recognition,"
IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 441–450, Sep.2009.

[29] X. Zhao and S. Zhang, "Facial expression recognition based on local binary patterns and kernel discriminant isomap," Sensors, vol. 11, no. 10,pp. 9573–9588, 2011.

[30] R. Jiang, M. Parry, P. Legg, D. Chung, and I. Griffiths, "Automated 3D animation from snooker videos with information theoretic optimization,"
IEEE Trans. Comput. Intell. AI Games, vol. 5, no. 4, pp. 337–345, Dec.2013.