Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Finger Print Matching based on Miniature and PHOG Feature Extraction

M. Malarvizhi
P.G. Student,
Dept. of Information Technology,
Vivekanandha College of Engineering for Women, Tamilnadu, India

M. Madlin Asha
Associate Professor,
Dept. of Information Technology
Vivekanandha College of Engineering for Women, Tamilnadu, India

S. Sinduja
Associate Professor,
Dept. of Information Technology,
Vivekanandha College of Engineering for Women, Tamilnadu, India

Abstract- Registration of fingerprints is employed for matching the fingerprint of the persons. The registration process are used to save the patterns of the fingerprints of each person and based on the identification of the similar patterns in the dataset,thus the persons were identified. In the usage for the authentication fingerprint is most commonly used in biometric. Fingerprints of each and every person is different and hence the authentication can be given more effectively using fingerprint. The extracted features were encrypted using RSA algorithm. The miniature points and PHOG features were extracted from the fingerprint for the extraction of the features. For the recognition of the fingerprint the classification is based on classifier, like Fuzzy Nearest Neighbor process can be used. The performance of the process can be measured based on the performance of the classifier used.

Index Terms- RSA, FNN, PHOG and Miniature

I. INTRODUCTION

Biometrics refers to the quantifiable data (or metrics) related to human characteristics and traits. Biometrics identification (or biometric authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics. More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information. "Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometrics identification has eventually a much broader relevance as computer interface becomes more natural.

A unified framework photo-response nonuniformity noise (PRNU) cannot be used for Device Identification[1], there is not really a fundamental difference between these two tasks as the noise residual from a single image can be considered as a poor-quality fingerprint[2], this would eliminate all the advantages due to storage and memory operations, computation of the matching metric will be fast[3], It does not permit us to characterize the measurements[4], PHoG (Pyramid Histogram of oriented Gradients) descriptor is mainly inspired by two sources: i) Use of the pyramid representation of Lazebnik et al and ii)Histogram of oriented Gradients of Dalal and Triggs. Here, PHoG descriptor is used as feature for representing the images which also impose grids of various resolutions on the image space can offer more efficient image matching [5].

a novel fast search algorithm are used some parameters that are mutually dependent, making it difficult to find a good combination[6]

Fingerprint identification, known as dactyloscopy, or hand print identification, is the process of comparing two instances of friction ridge skin impressions, from human fingers or toes, or even the palm of the hand or sole of the foot, to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand may be slightly different. Fingerprint identification, also referred to as individualization, involves an expert, or an expert computer system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to have originated from the same finger or palm. Friction ridge is a raised portion of the epidermis on the digits (fingers and toes), the palm of the hand or the sole of the foot, consisting of

one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis.

RSA algorithm is used to send the messages from the sender to the receiver without allow the thirty parties to hack the content of the messages. The key validation problem will be solved by the creation of KEGVER (KEy Generation with VErifiable Randomness) protocol used to avoid the problems. with respect to any known attack and unlikely to be stale. The RSA algorithm is indeed among the strongest, but it cannot withstand the test of time. In fact, no encryption technique is even perfectly secure from an attack by a realistic cryptanalyst.Methods such as brute-force are simple but lengthy and may crack a message, but not likely an entire encryption scheme.

II. PROPOSED ALGORITHM

In the proposed system,each image that is stored in the database has its features extracted and compared to the features of the input image. Figure 1 describes the pictorial image of the proposed system,the first step in the process is, the input fingerprint is taken. The features were extracted from the fingerprint using miniature feature extraction and PHOG features.The miniature feature extraction is helpful for the identification of the important ridges and corners in the input images. The PHOG features were extracted inorder to extract the texture based informations in the images.

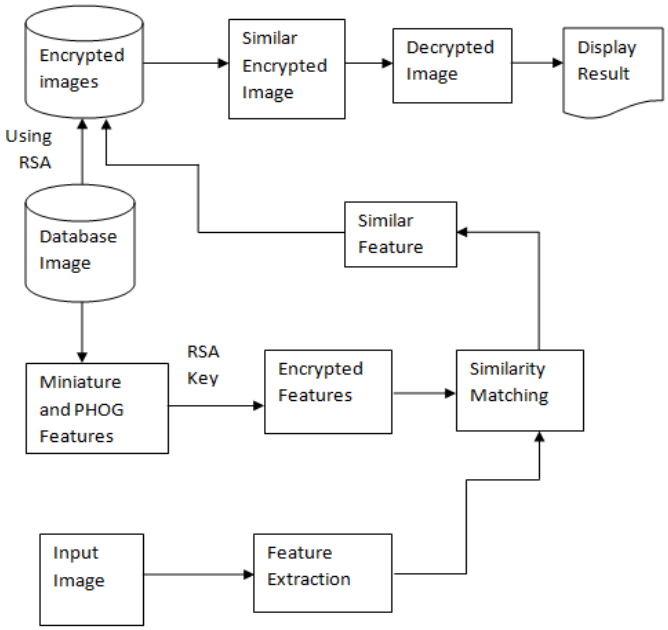

Figure 1: Block Diagram for Proposed System

The extracted features were then encrypted using RSA encryption method. The usage of the encryption process is helpful to keep the features more secure. The features were then decrypted to get the original features. Finally, these images from the database, as compared with the query image present in the database and then it display.

A) Image encryption using RSA algorithm

The RSA is an algorithm used by modern computers to encrypt and decrypt messages. The key used for encryption is different from (but related to) the key used for decryption. It is an symmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone, the other key must be kept private.

In case of public cryptography, we use one public key andone private key to send our message. But in this case we may have a chance to loss our content, to avoiding that we provide more secure and authentication by using two set of keys, One use as the sender's private key by using this we can encrypt the image and another key as the receiver's Public key by using this we provide the authentication. Then the receiver decrypt the encrypted image at the receiver side by receivers' private key and provide the authentication by sender's public key.

The steps involved in RSA double key image encryption algorithm is described below:

1. Choose two prime numbers p and q. (prime number is a number divisible only by that number and 1)
2. Set n equal to p * q.
3. Choose any random encryption key d, such that GCD (d, ((p-1) * (q-1)))=1
4. Find e such that e * d= 1 (**mod** ((p-1) * (q-1)))
5. Publish their public encryption key: PU={e,N}
6. Keep secret private decryption key: PR={d,p,q}
7. From the sender side, to provide the authentication we use the key as ep, it can be calculated as the form similar to the calculation of e, like ep. dp=1 mod ø(N) and 0≤d≤N
8. The receiver side we provide the authentication by using the private key as dp, by randomly.

1) Encryption Process

Encryption is the process of transforming information (called plaintext) into an unreadable form (called ciphertext) using an encryption algorithm combined with a parameter (called an encryption key). Only those who possess the decryption key can reverse the process and recover the original plaintext.The equation using private key (e) and the public key(ed)

$$C = M^e \bmod n \qquad (a)$$

$$E = C^{ed} \bmod n \qquad (b)$$

Compare the above equations (a) and (b) is

$$E=(M^e \bmod n)^{ed} \bmod n \qquad (c)$$

Where c represents a cipher text, M represents a message to be encrypted, n=pq, E represents the encrypted image**, e** represents private key and ed represents public key.

2) Decryption Process

Decryption is the process of converting the cipher (hidden) form into an original image, to know the actual content by the receiver. The receiver can decrypt the image by the private key (*d*) and provide the authentication by the public key (*dp*).

$$M = E^{d} \bmod N \qquad (d)$$

$$D = M^{dp} \bmod N \qquad (e)$$

The above equations (d) and (e) can be combined and rewritten as,

$$\mathbf{D = (E\ d \bmod N)dp \bmod N} \qquad \mathbf{(f)}$$

where *E* denotes the encrypted image, *d* denotes receiver's private key, *dp* denotes sender's public key and D denotes the resultant decrypted image.

B) Miniature Features

The input finger print images were initially trained by extracting features from images based on the miniature points from the images. The miniature points in the images were based on the features like Ridge ending – the abrupt end of a ridge. Ridge bifurcation – a single ridge that divides into two ridges. Short ridge, or independent ridge – a ridge that commences, travels a short distance and then ends. Island – a single small ridge inside a short ridge or ridge ending that is not connected to all other ridges. Ridge enclosure – a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge. Spur – a bifurcation with a short ridge branching off a longer ridge. Crossover or bridge – a short ridge that runs between two parallel ridges. Delta – a Y-shaped ridge meeting. Core – a U-turn in the ridge pattern. The features were obtained from the Ridges and bifurcations of the finger print.The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

C) PHOG Descriptor

In this paper, Pyramid Histograms of Oriented Gradients (PHOG) features are extracted from an image database as primitive features. PHOG descriptor is a spatial pyramid representation of HOG descriptor, and reached good performance in many studies. PHOG features are extracted from various samples to represent by their local shape and spatial layout. Each image is divided into a sequence of increasingly finer spatial grids by repeatedly doubling the number of divisions in each axis direction. The number of points in each grid cell is
then recorded. The number of points in a cell at one level is simply the sum over those contained in the four cells it is divided into at the next level thus forming a pyramid representation. The cell counts at each level of resolution are the bin counts for the histogram representing that level. For each grid cell at each pyramid resolution level, a HOG vector is computed. The final PHoG descriptor for the image is then a concatenation of all the HOG vectors. The intensity histogram shows how individual brightness levels are occupied in an image; the image contrast is measured by the range of brightness levels. The histogram plots the number of pixels with a particular brightness level against the brightness level. For 8 bit pixels, the brightness ranges from zero (black) to 255
(white).

III. EXPERIMENTAL RESULTS

ROC curve, is a graphical plot which illustrates the performance of a binary classifier system as its discrimination threshold is varied. It is created by plotting the fraction of true positives out of the total actual positives (TPR = true positive rate) vs. the fraction of false positives out of the total actual negatives (FPR = false positive rate), at various threshold settings. TPR is also known as sensitivity or recall in machine learning. The FPR is also known as the fall-out and can be calculated as one minus specificity.

True positive = correctly identified

False positive = incorrectly identified

True negative = correctly rejected

False negative = incorrectly rejected

$$\text{Sensitivity} = \frac{\text{TP}}{(TP + FN)}$$

$$\text{Specificity} = \frac{\text{TN}}{(FP + TN)}$$

This is sample ROC for the classification process.The inputs for the ROC curve is the predicted and the target values.The predicted values refer to the values recognized based on proposed method.The actual values refer to the original values for the input dataset. This denotes the correct labels for the classifier.The center line in gray lines denotes the exact classification rate and the blue color denotes the proposed classification rate. When the blue lines reaches the value 1 then the proposed method is 100% accurate.

IV. CONCLUSION

The proposed method is capable for the identification of the persons in a more accurate manner. The extracted features based on the different feature extraction methods were more reliable. The extracted features were encrypted inorder to keep it more secure.The encryption and decryption process is done based on RSA algorithm. The classification method used is increases the accuracy of the process since the classifier employs fuzzy logic and distance metric for the classification process. The performance of the process is measured using Accuracy, Specificity and Sensitivity.

REFERENCES

[1] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Determining image origin and integrity using sensor noise," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[2] M. Goljan, J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," *Proc. SPIE*, vol. 7541, pp. 754108-1–754108-12,Jan. 2010

[3] Y. Hu, C.-T. Li, Z. Lai, and S. Zhang, "Fast camera fingerprint search algorithm for source camera identification," in *Proc. 5th Int. Symp. Commun. Control Signal Process. (ISCCSP)*, May 2012

[4] L. Jacques, J. N. Laska, P. T. Boufounos, and R. G. Baraniuk, "Robust 1-bit compressive sensing via binary stable embeddings of sparse vectors,"*IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2082–2102, Apr. 2013.

[5] Anna Bosch, Andrew Zisserman, Xavier Munoz, , "Representing shape with a spatial pyramid kernel", ACM, July 09-11, 2007.

[6] Y. Hu, C.-T. Li, and Z. Lai, "Fast source camera identification using matching signs between query and reference fingerprints," in *Multimedia Tools and Applications*. New York, NY, USA: Springer-Verlag, 2014, pp. 1–24. [Online]. Available: http://dx.doi.org/ 10.1007/s11042-014-1985-3.

[7] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[8] J. Vybíral, "A variant of the Johnson–Lindenstrauss lemma for circulant matrices," *J. Funct. Anal.*, vol. 260, no. 4, pp. 1096–1105, 2011.

[9] J. Lukáš, J. Fridrich, and M. Goljan, "Determining digital image origin using sensor imperfections," *Proc. SPIE*, vol. 5685, pp. 249–260, Apr. 2005.

[10] M. Goljan and J. Fridrich, "Camera identification from cropped and scaled images," *Proc. SPIE*, vol. 6819, pp. 68190E-1–68190E-13, 2008.

