Asymmetric key generation using Ear biometrics

Amirtha Ganexan Shivram, G. Sundar, T. Tamiliniyan, S. Pavithra
1,2,3 UG Student, Department of ECE, Rajalakshmi Engineering College, Chennai.
4 Assistant Professor, Department of ECE, Rajalakshmi Engineering College, Chennai.

Abstract—Our modern day era faces an inevitable problem of securing our most integrated data and messages. The chief problem is to protect our data in a unique way that could only be worked upon by the sender and the recipient. Ear based Encryption is preferable biometric technique for securing text. In this paper it is proposed to use the details obtained from the human ear to put forth a new encryption method. The main reason behind choosing ear based encryption is the uniqueness and cannot be forged with ease. The phases involved are: image acquisition, preprocessing, feature extraction and generation of key. The features obtained from the ear are henceforth used to generate asymmetric key using RSA algorithm.

Keywords—Encryption, Human ear, RSA.

1. INTRODUCTION

Biometrics is the study of identification or authentication of individuals based on their physiological or behavioral characteristics. Traditional means of automatic recognition, such as passwords or IDs can be forgotten, stolen or forged. The features must be unique, permanent, collectable and measurable. Biometrics are used in different domains like robotics, administrative field line spacing, forensic identification, access and security control.

The characteristic appearance of external ear is formed by the outer helix, the antihelix, the tragus, the antitragus, the lobe and the concha as shown in (Fig.1). The shape of the outer ear evolves during the embryonic state. The influence of random factors on the ear’s appearance can best be observed by comparing the left and right ear of the same person. Even though the left and right ear show some similarities, they are not symmetric [1]. Recent studies even validate that certain features of the ear are distinct for identical twins [4]. This fact further implicates its applications in the field of security and puts ear images on comparison with epigenetic biometric modals, such as the iris.

Research about the changes in the appearance of the outer ear with time has shown that the ear changes slightly in size when a person ages [2]. A study on the effect of short periods of time on ear recognition [3] shows that the recognition rate is not affected by ageing.

The size of the ear is small so amount of image processing required is less when compared to object in large size. Processing of the ear image is simple compared to that of the iris or the distribution of minutiae in fingerprint identification. Features of the ear are fixed which implies less image processing work and saves time.

Fig.1. Structure of the outer ear.

Nowadays, police and forensic investigators use ear prints as a proof of identity [8]. As we see in (Fig.2), the convict’s ear is clearly visible and can be used for future identity confirmations and forensics. This has been very useful as in most countries ears have to be visible in photographs for passport and other IDs.

In this article, the unique and robust features of the human ear are used to develop a new cryptosystem. The existing implementation of ear biometrics are in the fields of passive person identification and authentication like the ones by M.Burge et al.[11], M. Rahman et al.[20] and V.K. Narendra Kumar et al.[9].

1.1 Ear Recognition

Techniques for automatic identity recognition from ear images can in general be classified based on either 2D or 3D ear data. Here, we primarily focus on 2D approaches and refer to other reviews, such as [5], for a detailed coverage on the 3D ear recognition approaches. A 2D ear recognition system operates on images or video footage captured with commercial cameras, surveillance systems or similar hardware. In a fully automatic setting, the system should first detect a profile face in the input
image and segments the ear from the detected region. Then the segmented portion is subjected to preprocessing. The purpose of preprocessing is to minimize the variation in the acquired image, while keeping the characteristic features of the subject intact. Different preprocessing methods are applied to 2D intensity data and 3D range data [6][9]. Features are extracted from the pre-processed image and identity recognition is conducted based on suitable classification technique. Depending on the type of feature extraction technique used, 2D ear recognition approaches can be divided into geometric, holistic, local and hybrid methods.

![Classification of 2D ear recognition approaches](image)

Geometric techniques exploit the geometrical characteristics of the ear, such as the shape of the ear, locations of specific ear parts and relations between these parts. Holistic approaches treat the ear as a whole and consider representations that describe the global properties of the ear. Local approaches describe local parts or the local appearance of the ear and exploit these descriptions for recognition. The last category of hybrid approaches covers techniques that do not strictly fit into any of the other categories and usually comprises methods that combine elements from all categories or rely on multiple representations to improve performance [10].

1.2. Cryptography

Cryptography is the study of hiding information using secret keys and sent via wired/wireless channel. Information sent may be text, number, image, audio or video. Various types of cryptography includes i) Public key cryptography, ii) Secret key cryptography and iii) Hash functions. Public key cryptosystem or asymmetric key cryptography uses two keys - public and private keys. Private key cryptosystem is otherwise known as symmetric/single key cryptography that uses one key that is known to both sender and receiver. If this key is disclosed, communications are insecure and are compromised. Hash functions uses single key and used for encryption.

1.3 RSA Algorithm

RSA cryptosystem was developed by Rivest, Shamir & Adleman of MIT in the year 1977. It is the best known and widely used public-key cryptography scheme. It is based on integer modulo of prime numbers. RSA algorithm provides better security due to cost of factoring large numbers. The steps in RSA algorithm are,

1. Key generation.
2. Encryption of plain text to produce Cipher text using public key.
3. Decryption of cipher text to obtain plain text using private key.

1.4 Biometric Crypto Systems

Although Cryptography is effective in secure transmission of data over an insecure channel, it also has significant drawbacks. The encrypted message is based on the key rather than user authenticity. For powerful encryption, the length of the keys used for encryption and decryption becomes quite large. But still the keys can be guessed or cracked by simple dictionary attacks. Moreover, the maintenance and sharing of such lengthy and random keys becomes a dominant problem in cryptography systems. These problems can be well tackled by using Biometric Cryptosystems. The integration of biometrics with cryptographic algorithms yields a much powerful crypto system known as biometric cryptosystem. It involves the use of both cryptography and biometrics to strengthen the encryption scheme. Such systems make use of the cryptographic level of security along with the uniqueness of the biometric traits of the user. Biometrics eliminates the need to remember the key or even its exchange over a network. In such a system, the key generation process involves the use of a biometric trait of the user.

The focus of this paper is the generation of cryptographic keys using human ear as the biometric of choice without compromising the privacy and security involved in the process of key generation.

2. CRYPTOGRAPHIC KEY GENERATION

A cryptographic key generation scheme is proposed through the following algorithm in which the efficiency lies in its ability to generate the key from the extracted points of interest from the human ear.

2.1 Preprocessing

The side profile image(s) of the user are obtained with the help of a digital camera. This image undergoes preprocessing and the region of interest is obtained i.e the ear. This is done through object recognition/detection techniques. Haar cascades are observed to provide effective results.
2.2 Binarization of the ear image

The binarization technique transforms the scanned digital image of the ear to machine interpretable values. Such a method checks each pixel value and compares it to the mean intensity value. If found greater, then the pixel values are changed accordingly. This is done for effective processing and feature extraction.

2.3 Contours and Edge detection

The edges and contours of the preprocessed image are determined. There are many techniques that can be used for this purpose like the OpenCV image processing modules. This is a simple technique through which the ear’s features can be extracted.

2.4 Key Generation

In the following section, a key generation system is depicted based on the algorithm using contours developed from the ear image. Inspired by number of related researches in the field of cryptography and biometric techniques, the algorithm proposed is represented below. The same is represented in Figure 6.

Steps involved:
Step 1: Edge detection and obtaining contours

Step 2: Calculating the areas of the possible contours.
   - Rect = Area of minimum rectangle
   - Box = box points
   - Radius = minimum radius of enclosing circle.

Step 3: Obtaining two prime numbers from the above determined parameters. This can simply be done by summing up all the above parameters and finding the next prime number of the sum.
   - Prime1 = (first prime number)
   - Prime2 = (second prime number)

Step 4: The prime numbers obtained from the previous step are given as inputs(P & Q) to the RSA algorithm.

Step 5: Generation of public and private keys.

Thus the key generated using the above mentioned algorithm generates both public and private key using features extracted from an individual’s ear. On the basis of the experimental results, it may be inferred that an attacker, in case of a biometric cryptosystem, will be unable to generate a similar key.
but fake key without having the complete knowledge of the algorithm generating the key and the individual’s ear.

3. RESULT AND CONCLUSION

The proposed ear based method yields the better biometric system. This method is simple and efficient to implement. The processing overhead is also less when compared to face, iris or fingerprint based cryptosystems. The proposed method can be well utilized in mobile phone based banking and other information security applications.

4. REFERENCES
