Advanced Security Measure for Mobile Authentication

Satendra H. Mane
Associate Professor,
Dept. of Electronics & Telecommunication
Padmabhushan Vasantdada Patil Pratishthan's College of Engineering,
Sion,Mumbai-400 022
mane.satendra@gmail.com

Rajesh B. Morey
Assistant Professor,
Dept. of Electronics & Telecommunication,
Padmabhushan Vasantdada Patil Pratishthan's College of Engineering,
Sion,Mumbai-400 022
raju1000@rediffmail.com

Rajiv S. Tawde
Lecturer,
Dept. of Electronics & Telecommunication,
Padmabhushan Vasantdada Patil Pratishthan's College of Engineering,
Sion,Mumbai-400 022
rajiv1186@gmail.com

ABSTRACT

In this paper, we present a new method for mobile authentication by Main Switching Centre (MSC). In the recent time, it has been observed that one can make a duplicate SIM (Subscriber Identity module) card of existing SIM card, more ever, one can get a SIM card easily by providing fake documents and can make misuse of such SIM cards. In this method, we propose to use biometric identifier finger-print and signature for authentication of mobile-station. If a person wants to buy a SIM card, then he or she has to provide his or her finger-prints and signature to the service provider.The finger-print is collected with the help of optical sensor and the signature can be collected with the help of resistive or capacitive touch screen pad.The service provider will store the digitized finger-print image and the digitized signature of the user, both in the SIM card and the Home location register (HLR). Before availing network to the mobile station, the Authentication Center (AuC) will first verify the finger-print and signature of the user. If it matches, then only the user will be allowed to use the network. It has been proved that every person has a unique finger-print and signature pattern.The signature and the ridge frequency variation can be converted into a digital value and this unique digital value can be used as a cryptography key for transmission of plain text data originating from the mobile station.

Keywords

Biometrics, Authentication center (AuC), Ridges,Valleys, Signature, Ridge frequency, Cryptography key K_c ,Global system for mobile (GSM) .

1. INTRODUCTION

Mobile communication is a wireless communication, in which information signal is transmitted and received via the air. Hence security and privacy is uttermost important for faithful and safe transmission and reception of the signal. Normally, we have two types of mobile systems, viz. Global system for Mobile (GSM) and Code Division Multiple Access (CDMA).

GSM phones make use of SIM cards in which we store information like Authentication key (K_i), User International Mobile Subscriber Identity (IMEI), Algorithm A3 for authentication, Algorithm A8 for generating Cryptography key (K_c), etc. Each user gets a unique key K_i which is stored in the SIM card. The K_i is a 128-bit number which is paired with IMSI number when the SIM card is created. The K_i is only stored in the SIM card and in the Authentication center (AuC) in the MSC and it is never transmitted across the network on any link. Whenever the user requests for the network, then AuC generates a 128-bit random number RAND. During the authentication process, mobile station receives this number from the MSC and then this RAND number is used by the SIM card to generate signal response (SRES). SIM card generate the SRES with the help of Algorithm A3 stored in it. The SRES is a 32-bit number. Normally many GSM administrations use a common A3 which is available from the GSM-MOU (Memorandum of Understanding). The SRES number generated by the Mobile station goes to AuC where AuC verifies it.[1]

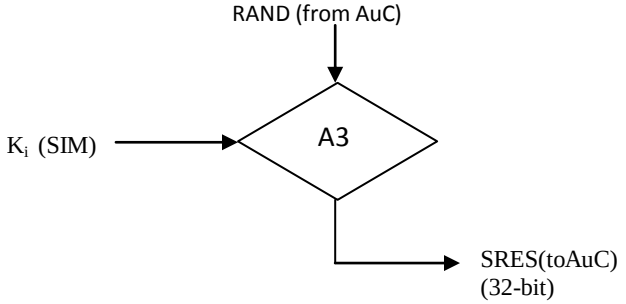

Fig 1: A3 algorithm flowchart.

Once the mobile phone passes the A3 algorithm test, then it can use the network for voice transmission. Then the mobile station uses RAND received from the network and mixes with K_i through an algorithm called A8 and generates cryptography key K_c, which is 64-bit. The algorithm A8 resides on the SIM and on the AuC.

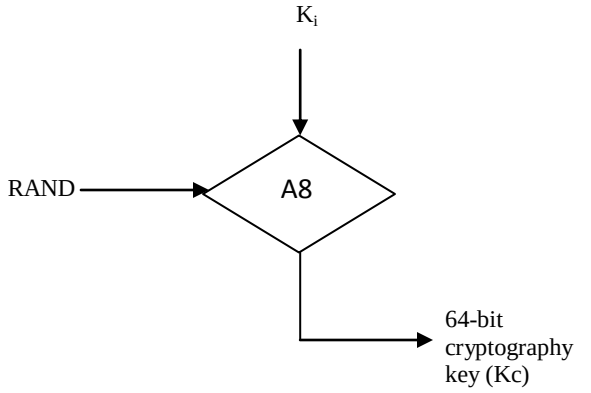

Fig. 2: A8 algorithm flowchart

Finally the encryption algorithm is used to encrypt the data which is being transmitted on the network. This is done with the Algorithm A5. The two inputs to the A5 algorithm are K_c and plain text data. The A5 algorithm is present in the mobile equipment and it is not a part of the SIM card.[1][3]

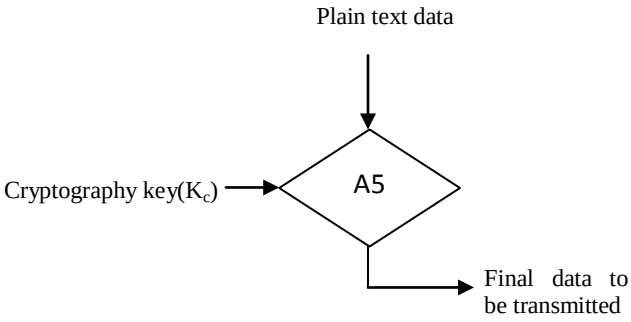

Fig.3 : A5 algorithm flowchart

2. Finger print analysis and representation

In recent times, it has been observed that this method of authentication has failed and is inadequate. Moreover, it is also observed that by simply providing documents of dead person, one can easily avail a SIM card in the name of the dead person which is a crime. Such SIM cards can be mis-used. Hence, in order to have more promising authentication methods, we suggest to involve biometric parameters like finger-print and signature. Before issuing SIM card to the user, the dealer has to collect two biometric information ,viz. finger-print and signature. A biometric is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioral characteristics possessed by that person. The common biometrics which we can use are DNA, ear, face, gait, iris, signature, retinal scan, etc. Fig. 4 shows a finger-print image. A finger-print is the reproduction of a finger-tip epidermis, produced when a finger is pressed against a smooth surface. The most evident structural characteristics of a finger-print is a pattern of interleaved ridges and valleys; in finger-print image, ridges are dark, whereas valleys are bright. Ridges vary in width from 100µm, for very thin ridges to 300µm for thick ridges. Generally, the period of ridge/valley cycle is about 500µm. Injuries such as superficial burns or cuts do not affect the underlying ridge structure and the original pattern is duplicated in any new skin that grows. Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate. When analyzed at the global level, a finger-print pattern exhibits one or more regions where the ridge lines assume distinctive shapes. These regions are known a singular regions and may be classified into three topologies, viz. loop, delta and whorl. Several finger-print matching algorithms pre-align finger-print images according to a landmark or a center-point called the core. The core is defined as the northmost point of the innermost ridge line. At the local level, other important features called minutiae can be found in the finger-print patterns. Minutiae means small details and it indicates the various ways that the ridges can be discontinuous e.g. A ridge can suddenly come to an end or can divide into two ridges, etc. Each minutiae or the ridge pattern can be denoted by its class, the x- and y-co-ordinates and the angle between the tangent to the ridge line at the minutiae position and the horizontal axis.

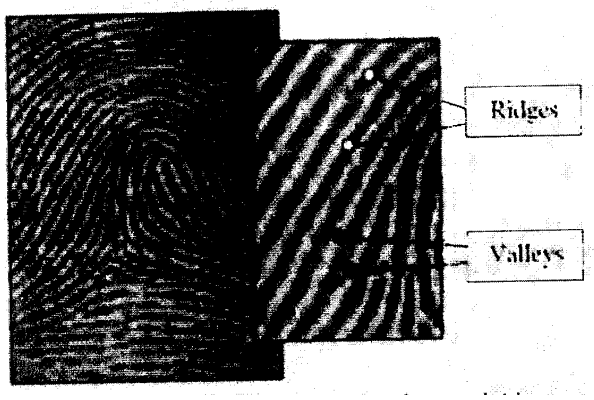

Fig.4(a): Ridges and valleys on a finger-print image.[2]

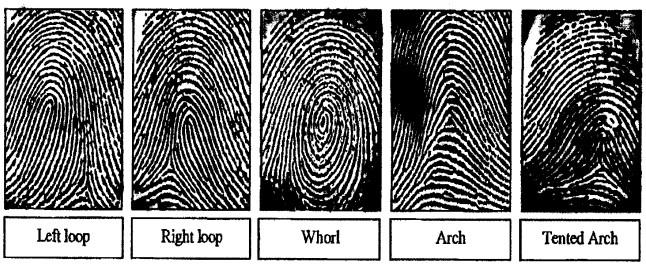

Fig.4(b) : Major classes of finger-print.[2]

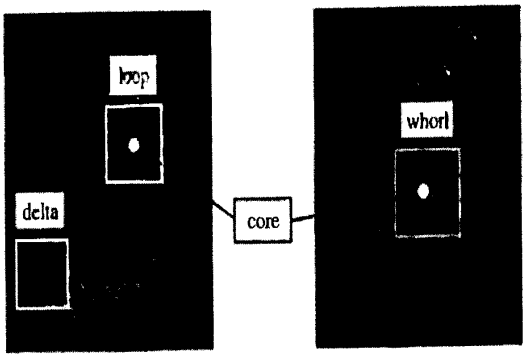

Fig. 4(c): Singular regions and core points in finger-print images[2]

3. Storing and compressing finger-print image

The finger-print image can be captured with the help of optical sensors like FTIR (Frustrated total internal reflection) sensor. Each finger-print impression, when digitized at 500 dpi, produces an image of 768 X 768 pixels at 256 gray levels. Such image will require 10Mb of memory for encoding purpose. To avoid this problem, we can use wavelet scalar quantization (WSQ) in which the finger-print image is decomposed into a number of spatial frequency sub-bands (typically 64) using a discrete wavelet transform. Then resulting coefficients are quantized. Then the quantized sub-bands are concatenated into several blocks and compressed using an adaptive Huffman runlength coding. After compression, we can store the digital value into the memory of the SIM card and in AuC of MSC.

4. Signature acquisition and storing

Signatures are captured using a touch-screen. As shown in Fig. 5 and 6, a resistive touch-screen consists of two layers separated by an air-gap. The layers are made of indium tin oxide. The upper layer has connecting strips on top and bottom. The lower layer has connecting strips on right and left. There is a protective covering of glass or acrylic to protect the layers. The resistance of both the layers is about 100Ω to 300Ω. Normally we apply dc voltage of +5V to both x and y plane. The voltages are applied alternately to x & y plane with a delay of 100µs. When a person puts his/her signature on the touch screen with the help of stylus, then it generates a continuous time-varying signal, both on x+ & y+ pins of touch screen. This analog voltage is then converted into digital form with the help of ADC. This digital value is then stored in the memory of the SIM card and also in the AuC of MSC. [5]

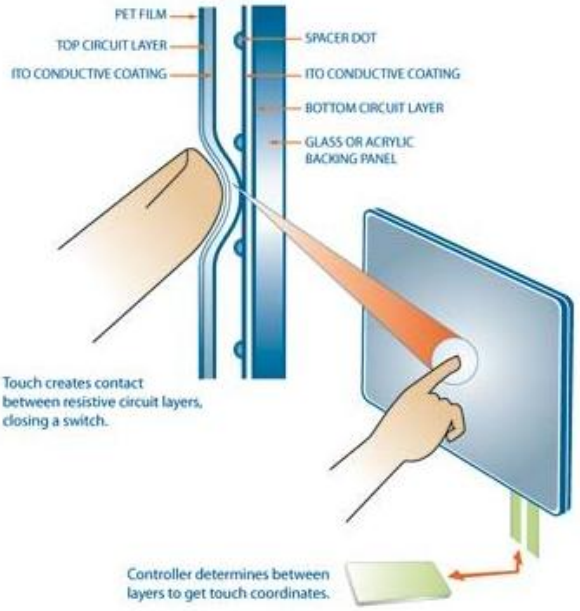

Fig. 5: Touch-screen for signature acquisition. [5]

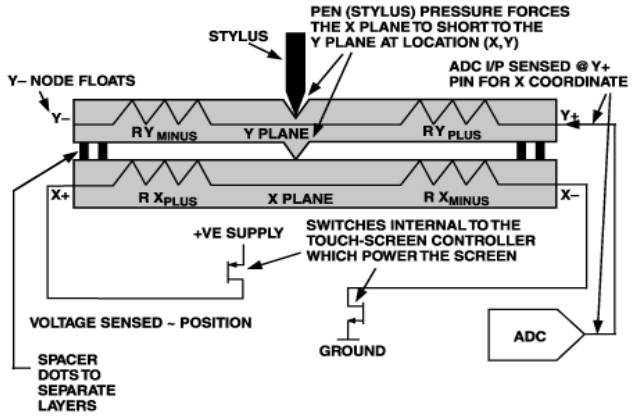

Fig. 6: Electrical diagram of touch screen with a stylus.[5]

5. New method for authentication of mobile station

As per our authentication method, for an individual user, the binary value of the finger-print & signature is stored both in AuC and in the SIM card and we have to design the A3 algorithm in such a way that during the authentication process, we will have finger-print & signature verification, and if the binary value of the finger-print and signature stored in the SIM card matches with the value in the AuC, then only 32-bit SRES number will be generated and then only MSC will assign voice channel to the mobile phone.

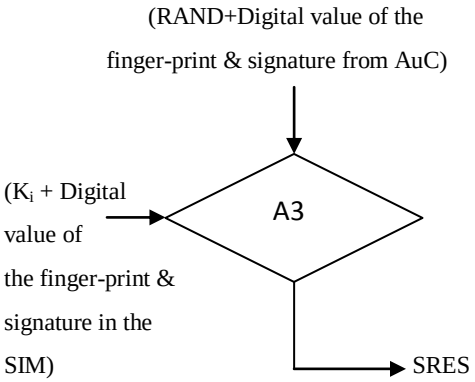

Fig 7: A3 Algorithm with finger-print & signature verification.

As shown in Fig. 8, the K_i bit and RAND is given to algorithm A8 which generates the cryptography key K_c.

The binary value of K_c is again EX-ORed with the binary value of finger-print and signature to generate a new cryptography key K_c'. The K_c' can be used as a PN-sequence and it is mixed with the plain text data before transmission. Thus, if we are transmitting the plain text data with encryption of new cryptography key K_c', then even if anybody hacks the signal, then it will provide a better protection, privacy and security.

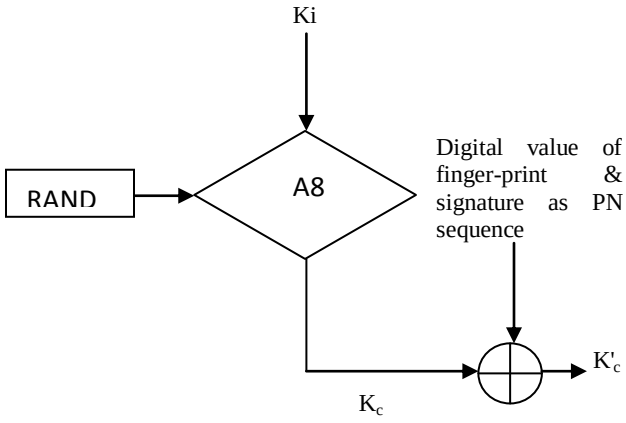

Fig. 8 : Flowchart for generation of K'_c

Thus if we are transmitting the plain-text data with encryption of new Cryptography key K'_c ,then even if anybody hacks the signal then it will provide a better protection against unauthorized listening, this is because the K'_c is having a unique binary number which depends upon the user's finger ridge frequency variation and signature pattern of the user.

CONCLUSION:

Thus, with the old mobile Authentication Algorithm, if we add finger-print matching and signature verification, then it will be difficult for anybody to make a duplicate SIM card. A compulsion of finger-print & signature at the time of issuing a SIM card, will not allow anybody to purchase a SIM card in the name of a person who is dead. If we want to make this authentication still more promising, efficient and secured, then with finger-print & signature, we can make use of another biometric identifier like Iris and DNA.

REFERENCES:

[1] Rappaport,Wireless Communications - Principles And Practice, 2/e,Pearson Education,India.

[2] David Maltoni,Dario Maio,Anil K. Jain,Salil Prabhakar;Handbook of Fingerprint recognition,Springer.

[3] http://www.gsmfordummies.com/encryption/encryption.shtml

[4] http://en.wikipedia.org/wiki/biometrics

[5] http://en.wikipedia.org/wiki/resistivetouchscreen