INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

BANK AUTHENTICATION USING EL-GAMAL DIGITAL SIGNATURE AND BIOMETRIC HAND FEATURES

Dr. Saad Abdual azize

saadabdualazize@yahoo.com
Al Maamon College University, Computer science dept.

Abstract: - The human body has its own features like fingerprint, iris, face and smell; which used for finding the characteristics and behavior of the body. Fingerprint was one of the first ways used to find these characteristics. In this research the hand features are used with a public key algorithm for bank verification system.

Keywords: key generation, hand geometry, digital signature.

Introduction

Cryptography and biometrics are combined in biometric cryptosystem [1]. Biometric key system can be used generally in two different ways, biometric based key generation and biometric matching.

Biometrics comprises methods for exceptionally recognizing humans based upon one or more fundamental physical or behavioral personality. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance [2].

Biometric systems may be a distinct option for information based client confirmation techniques in light of the fact that biometric attributes are more firmly bound to a man than PINs and passwords are and can't without much of a stretch be overlooked or went on to other individuals, be it purposefully or inadvertently. Biometric information regularly contains data past what is required for verification, which one might want to keep private [3].

Digital signature

An advanced signature will be a scientific plan to demonstrating the legitimacy of advanced message alternately documents. A substantial advanced mark provides for a beneficiary motivation behind with think that those message might have been made toward referred sender, that those senders can't deny ‘hosting sent’ those message (authentication What's more non-repudiation), Also that those messages might have been not modified through travel (integrity). Advanced marks would regularly utilized for programming distribution, money related transactions, also on different other situations [4]

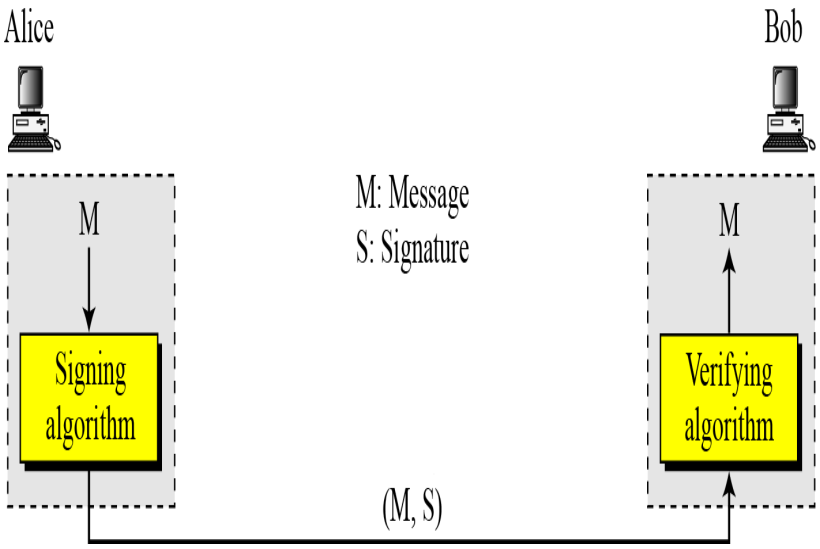


Figure1: Digital signature process

El-Gamal digital signature scheme

M: Message — r: Random secret
S_1, S_2: Signatures — d: Alice's private key
V_1, V_2: Verifications — (e_1, e_2, p): Alice's public key

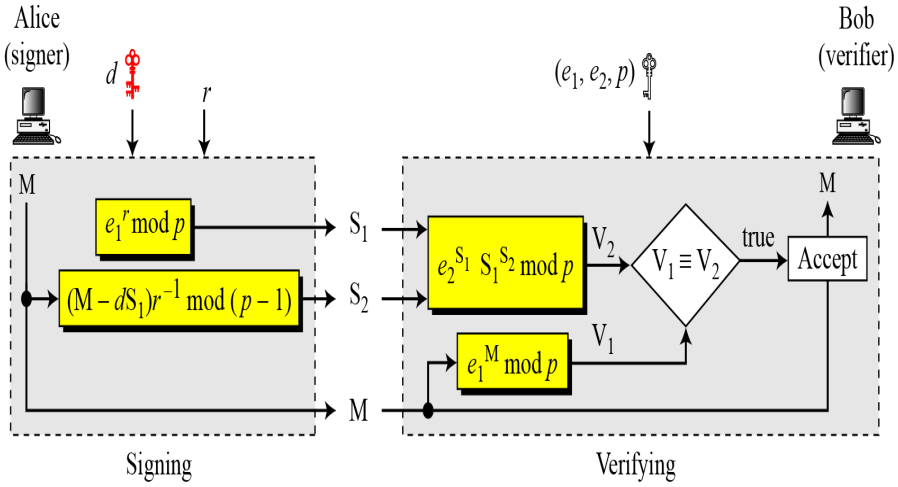


Figure2: El-Gamal digital signature scheme

El-Gamal encryption algorithm is not commutative however a closely related signature scheme exists. Security depends on the difficulty of computing discrete logarithms.

El Gamal Signature algorithm:

To sign a message M:

Each user (e.g., A) generates his/her key

1- Given a large prime p and its primitive root a
2- A chooses a private key: $1 < x < p-1$
3- A computes his public key: $y = a^x \bmod p$
   Hash m = H(M), $0 <= m <= (p-1)$
4- Choose random integer K with $1 <= K <= (p-1)$ and $\gcd(K,p-1)=1$ (K is the per message key)
5- Compute $S1 = a^K \bmod p$
6- Compute K^{-1} the inverse of K mod (p-1)
7- Compute the value: $S2 = K^{-1}(m-xS1) \bmod (p-1)$
8- If S2 is zero, start with a new k
9- Signature is:(S1,S2)

Any user B can verify the signature by computing

1- $V1 = a^m \bmod p$
2- $V2 = y^{S1} S1^{S2} \bmod p$
3- Signature is valid if V2 = V1
   $(a^x)^{S1} (a^K)^{S2} = a^{xS1+KS2} = a^{axS1+m-xS1} = a^m$

When signing a message, again create and "protect" a temporary signing key, then use it to solve the specified equation to create the signature. Note that M here is usually the hash of the actual message. Verification consists of confirming the validation equation that relates the signature to the (hash of the) message.

The Proposed Algorithm

The proposed algorithm that mix the hand biometry features with El Gamal algorithm was applied on banking system which needs the most secure signature method to be used in transactions, opening accounts and money transfer. The customer's hand image will be used to create his own signature. The proposed algorithm has two phases:

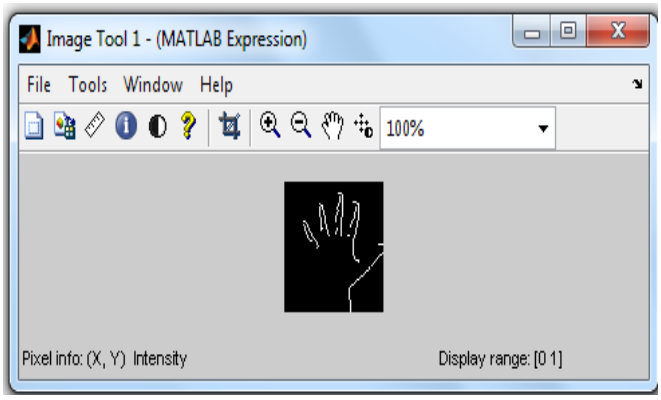
Phase 1: When making a request from the customer for the purpose of opening an account.

1- Scan the customer hand image and convert to gray scale.
2- Apply the canny edge detection.
3- Label each edge by a number.
4- Take the upper and lower point for each of the four fingers then find the distance.
5- Add the four distances and multiply by half to get one number.
6- If the number is not a prime, approach to the upper prime number (p).
7- Find the first primitive root number for total of distances (a).
8- From the first finger, find the first even (location) number (x)
9- Let (m) is the security number of the credit card.
10- From the second finger, find the first prime (location) number (k).
11- Calculate v2.
12- Save the number of the customer credit card and the calculated v2 to be used for later verification.

Phase 2: Customer makes deposit and withdraw processes

1- Enter the credit card security number (m).
2- Scan the customer hand image and convert to gray scale.
3- Apply the same steps of phase 1 (2-7) to calculate a new value (v1).
4- If v1 = v2 then complete the deposit or withdraw operation.

Implementation



Distance of first finger =17.02
Distance of second finger =18.3
Distance of third finger =22.2
Distance of fourth finger =19.4
p=1901
a = 85
X = 14
M = 7
K = 13
$Y = a^x \bmod p$
$Y= 85^{14} \bmod 1901$
Y= 1852

$r = a^k \bmod p$
$r=85^{13} \bmod 1901$
r=648
$s=k^{-1} (m-x*r) \bmod p-1$
s=877(7-14*648) mod 1900
s=1495

$v1= a^M \bmod p$
$v1=85^7 \bmod 1900$
v1= 375

$v2== y^r r^s \bmod p$
$v2=1852^{648} * 648^{1495} \bmod 1901$
v2=375
v1 = v2

Conclusion

There are thousands of ways to steal money from banks illegally; there are many ways to discover for the purpose of minimizing these breakthroughs, and the more complications on the way for withdrawing money. What is familiar is that, most of banks rely on the Visa card number especially in ATM machines. The proposed algorithm presents a more secure and authentic way for verifying the customer anywhere by not just entering the credit number but also by scanning the hand of the customer which cannot be forged. The proposed method used the biometric features of the customer hand to calculate the verification key used with El Gamal signature which gave it more strength. This method could be used in many fields not only bank transactions, like door opening and logging in to secrete files.

REFERENCES

[1] Wenbo Mao, Modern Cryptography Theory and Practice, Hewlett-Packard Company, Prentice Hall, July 25, 2003.
[2] ALAN G. KONHEIM, COMPUTER SECURITY AND CRYPTOGRAPHY, John Wiley & sons, inc ,2007.
[3] William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE, Prentice Hall.2011.
[4] J. Hofer, C. Gruber, and B. Sick., Biometric analysis of handwriting dynamics using a script generator model. In IEEE Mountain Workshop on Adaptive and Learning Systems,
Pages 36–41, Logan, UT, USA, 2006.
[5] Chan, C.K., Cheng, L.M., 2004. “Hiding data in images by simple LSB substitution”. Pattern Recognition 37 (March), 469–474.
[6] Deepesh Rawat , Vijaya Bhandari, 2013, “A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image “. International Journal of Computer Applications (0975 – 8887), Volume 64– No.20.
[7] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science,www.liacs.nl/home/tmoerl/privtech.pdf
[8] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001