Multimodal Biometrics Cryptosystem using Elliptic Curve

Ghada Abdelhady[1], Mohammed Ismail[2], Hussam Elbehiery[3]

[1.] Department of Computer networks, Faculty of Computer Science, Ahram Canadian University, Egypt
[2.] Department of Engineering Mathematics, Faculty of Engineering, Benha University, Egypt
[3.] Department of Computer Science, Faculty of Information Technology, MUST University, Egypt
ghada.abdelhady10@gmail.com

Abstract: Banks use encryption methods all around the world to process financial transactions and to protect their customers ID numbers at bank automated teller machines (ATM). Banks, all over the world, use symmetric ciphering algorithms like TDES to process financial transactions. These involve transfer of huge amount of money from one bank to another. Recently, Biometric ATM's are the latest inventions to help us avoid fraud and duplication. If somebody steals our card and knows our PIN, they can easily withdraw cash from our account. In case of biometric ATM's they cannot. Usually the PIN for bio ATM's is the finger print of the cardholder or his eye retina scan etc. These cannot be duplicated and hence they are very safe and secure. This paper will present a multimodal system for encryption and decryption data, any types of data received via a network in Banks. So by the end of this paper we get a biometric ATM prototype including different levels of security using biometric encryption. Besides that, our module presents a new symmetric system that will bring the simplest symmetric algorithm (DES, Data Encryption Standard) to the life. This system is called DES-EC as it is modified DES using the elliptic Curve (EC).

[Ghada Abdelhady, Mohammed Ismail, Hussam Elbehiery. **Multimodal Biometrics Cryptosystem using Elliptic Curve**. *J Am Sci* 2014;10(9):120-124]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 16

Keywords: ATM, Biometrics, DES, DES-EC,TDES,Elliptic Curves,Symmetric encryption.

1. Introduction

Biometrics is a technology that strives towards identifying or authenticating the identity of a living person based on biological key that make the process definitive and effortless. A person's live biometric data is being matched against a bio print in the database, such as a smart card. If it matches, it means that the person is who he or she claims to be and access is granted. This process is called verification. Using the password in one to many systems is checking against a full database of passwords. This process is called identification. The system only cares if the password is valid one, not if the person using the password is authorized to use it.

Biometric Encryption is a best method to secure our data and information. It guarantees the identification and authentication of the encryption process. To implement this technology, a powerful mathematical is used which known as Ciphering.

Ciphering algorithms can be divided into two categories: private-key (symmetric) and public-key (asymmetric). Private-key systems use a common private key shared between the communicating parties, while public-key do not require any key exchange [2]. The implementation of ciphering systems presents several requirements and challenges. First, the performance of the algorithms is often crucial. One needs encryption algorithms to run at the transmission rates of the communication links. Slow running cryptographic algorithms translate into consumer dissatisfaction and inconvenience. On the other hand, fast running encryption might mean high product costs since traditionally, higher speeds were achieved through custom hardware devices. In addition to performance requirements, guaranteeing security is a formidable challenge.

Our study will present a new algorithm that will be added to the known symmetric encryption algorithms. This system is called New DES based on Elliptic curve. It has the benefits of DES and also the benefits of Elliptic Curve Cryptosystem (ECC) as a public key algorithm. It has the simplicity of DES algorithm also it has the strength of ECC. Except that the key in ECC is a public key but the key in our new algorithm is still private and generated by a new technique mentioned in details in [1]. Also we will use different keys as we are going to use three biometric scanners, Fingerprint, retina and iris scanners. Biometric Encryption is the most suitable method to secure our data and information, in which the security is forced to check the incoming objects by scanning of our body and the scanned objects are stored in database as an image. Then, the stored images are compared with the original image that already stored in database.

The coming sections explain History and state of the art, how DES is modified to be secured. Also, we explain the flowchart of our system and the proposed prototype pictures. The last section demonstrates industry and market analysis including

the comparison between Multimodal Biometric ATM using EC and Biometric ATM using TDES which is currently used over world.

2. History and State-of-the-Art

Let us go to one of the symmetric-key algorithms as DES, TDES, AES and recently, DES-EC (New DES based on Elliptic Curve) used in our study. Most of them are easy and fast in hardware implementation and also they are so flexible in software. Thus, software-based systems would seem to be a better fit because of their flexibility [3]. Fortunately, many embedded processors combine the flexibility of software on general-purpose computers with the near-hardware speed and better physical security than general-purpose computers. Embedded processors are already an integral part of many communications devices and their importance will continue to increase. If we combine this with their flexibility to be programmed and their ability to perform arithmetic operations at moderate speeds, it is easy to see that they are a very promising platform to implement cryptographic algorithms [4] and [5].

The theory of operation of DES-EC was appeared for the first time in my publication by the end of 2010. DES-EC tried to bring back DES to life using elliptic curves which are considered the simplest possible curves after lines and conics. Elliptic curves over finite fields provide an inexhaustible supply of finite abelian groups. Such curves involve elementary arithmetic operations that make it easy to implement (in either hardware or software) [6]. They are generally more secure than others are. Elliptic curves could easily be applied to DES to improve its performance and make it hard to be broken. This paper presents a new symmetric algorithm using the Fiestel function and S-boxes like DES but each stage in this algorithm will be based on elliptic curve (EC) so it is called "New DES based on EC". DES-EC will be explained in the following section.

The word biometric refers to technologies that utilize specific human characteristics (specifically, biological features that are unique to each individual) to establish the identity of a person, or gain access to secure areas. Various devices of this type began to be developed in earnest after 9/11 and have continued to grow in popularity.

There are many types or devices for biometrics including: Fingerprint Scanner, Retinal Scanner, Facial Recognition, Voice Recognition, and Keystroke Recognition.

Security based on biometrics is commonly used to limit access to only certain individuals. This is useful for safeguarding information in government and corporate environments. Biometrics can also be used to identify people who do not wish to be detected. Biometric recognition or authentication refers to the automated method of verifying a match between two human biometric like fingerprints.

3. DES-EC: New DES based on Elliptic Curve

DES-EC depends on three stages: the plaintext masking stage, new key schedule stage and New S-boxes, as shown in figure 1.

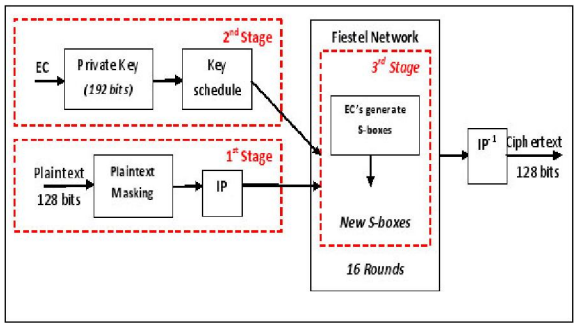

Fig.1. DES-EC Encryption Stages.

We notice in figure 1 that each stage will be based on EC or groups of EC's. Since the new algorithm is symmetric like regular DES, the structure presented in figure 1 is shared by the encryption and the decryption algorithms but in opposite directions. Meaning that the third stage represents the first stage after applying the inverse permutation and the first stage represents the last stage that includes the initial permutation and the inverse of the plaintext masking. The details of each stage are explained in [7] and [8].

As AES is the most widely used symmetric cipher today, so we present a theoretical comparison between the presented new algorithm "New DES based on EC" and AES. A comparison has been conducted for the encryption algorithms at different settings of the efficiency for each algorithm such as the key size, block size, and execution time for encryption and decryption algorithms shown in table 1. Average time required for exhaustive key search for DES, AES and the proposed algorithm New DES based on EC, is shown in table 2.

Table 1.New DES based on EC vs. TDES and AES

Key size (bits)	No. of Alternative keys	Time required at 1 decryption/μs	Time required at 10^6 decryption/μs
56 (DES)	$2^{56}=7.2*10^{16}$	2^{55}μs=1142 years	10.01 hours
128 (AES)	$2^{128}=3.4*10^{38}$	2^{127}μs=$5.4*10^{24}$ years	$5.4*10^{18}$ years
192 (New DES)	$2^{192}=6.3*10^{57}$	2^{191}μs=10^{44} years	10^{38} years

Table 2. Average time required for exhaustive key search

	DES	New DES	TDES	AES
Key size	56 bits	192 bits	168 bits	192 bits
Effective Key size	56 bits	127 bits (min)	168 bits	192 bits
No. of rounds	16	16	16	12
Block size	64 bits	128 bits	64 bits	128 bits
Strength	Non secured	secured	secured	secured

3.1 Elliptic Curves (EC)

All the EC's used in this study defined on a prime finite field Fp that is popular for EC used in cryptography [5]. The simple form of EC equation defined in Fp is shown in equation (1).

$$(y^2) \bmod p = (x^3 + ax + b) \bmod p \quad (1)$$

where a, b are constants and p is the order of the prime finite field Fp .Note that the right-hand side is a special cubic polynomial. The usage of elliptic curve in cryptography also requires that the curve be non-singular. Geometrically, this means that the graph has no cusps or self-intersections. Algebraically, this involves calculating the discriminant shown in equation (2) in order to prevent repeated roots on the right-hand side [9]. Equation (2) states that the curve is non-singular if and only if the discriminant is not equal to zero.

$$(4a^3 + 27b^2) \bmod p \neq 0 \quad (2)$$

Despite their simple form, elliptic curves have been studied for many years and have many significant applications in mathematics. Maybe one of the most interesting results related to the application of elliptic curves is that they are used to prove Fermat's Last Theorem [9]. Beside that they are the corner stone of Elliptic Curve Cryptography, ECC. ECC is particularly beneficial for application where:

- Computational power is limited (wireless devices, PC cards)
- Integrated circuit space is limited (wireless devices, PC cards)
- High speed is required [2].
- The properties of elliptic curves, defined on F_p, to generate points used in encryption have been presented in [10].

4. Biometrics scanners

There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device including location, security risks, task (identification or verification), expected number of users, user circumstances, existing data, etc [11].

5. Multimodal Biometric ATM

TDES is the ciphering algorithm that is applied in ATM over world to encrypt the customers' accounts. The block diagram of Biometric ATM which is applied for one scanner (fingerprint) that is commonly used is shown in Figure 2. The block diagram is considered as the proposed block schematic of crypto biometric authentication system using fingerprint scanner. It will be repeated for the other scanners (Iris and Retina) used in the suggested work.

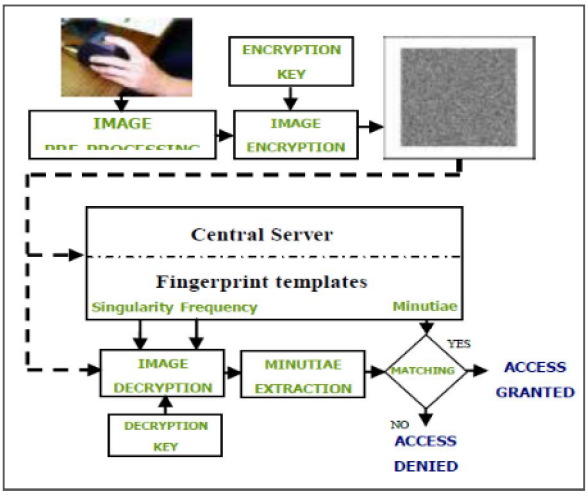

Fig.2. Schematic of embedded crypto biometric authentication system

Using biometric measures will enhance the security of ATM banking. As PIN-based ATM, machines are more secure than Biometric-based machines from the point of view of resistance to coercion crimes, Biometrics are used side by side with PINs and the system is able to detect and block emulation attacks. In our study, the encryption key will be used as a pass code for the first stage of the authentication as shown in the previous figure.

In our country, it is urgent to use more secured ATM using the unique features as the biometrics that it is not easy to be attacked. In addition, the proposed system classifies the security levels according to the required amount and its percentage from the whole account of each customer. The details of the proposed system are explained in the following block diagram shown in figure 3.

5. Multimodal Biometric ATM Prototype

The main target in our study is the achievement of the security. Also get a prototype for a multimodal biometric ATM with multi-level of security. Security is not accomplished by encryption alone. While the choice of encryption algorithms and key management routines are critical, they are

usually not the weak link in a secure application, Methodology and Execution Plan.

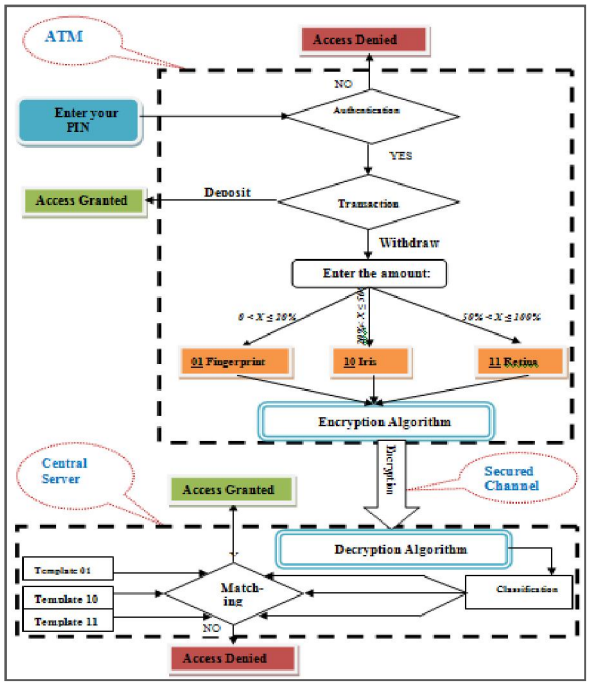

Fig.3.Multimodal Biometric ATM Block diagram

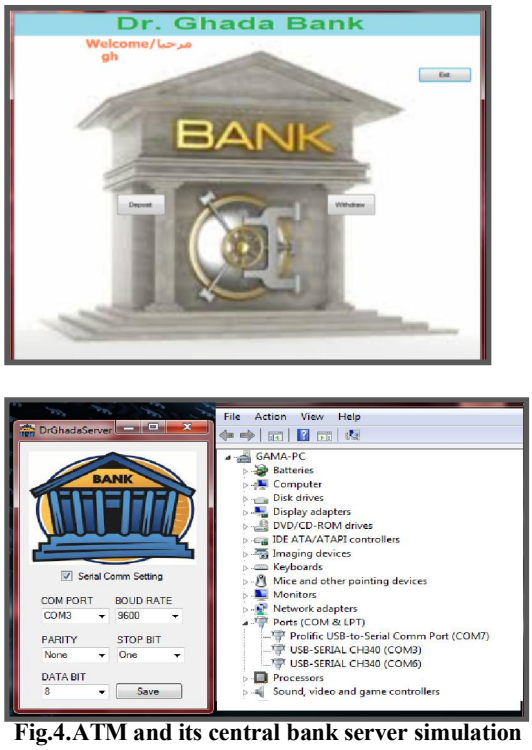

Fig.4.ATM and its central bank server simulation

In this system, we should have two expected states (Deposit and withdraw) to complete the transaction process. The user will Scan three biometric scanners according to the required amount in withdraw state, Figure 4 presents a simple graphical user interface to simulate the biometric ATM and the central server bank.

6. Industry and Market Analysis

Most of ATM over world uses TDES to encrypt the information of banking accounts. Although AES is more secured than TDES, TDES is used in ATM Banking, that is because the real time elapsed in TDES to encrypt or decrypt data is less than the time elapsed by AES.

In the proposed system, we impose new secured system to encrypt the banking data and the transactions according to the required level of security. Also in this study, we have three scanners for identifications rather than the one biometric scanner that is almost using the fingerprint. Our system uses three Biometric scanners applied during the transaction processes according to the required percentage of the total amount for the customer. Beside that the proposed system includes acknowledgment process to send a message to the customer cell phone before and after the transaction process to inform his/her the details of the transaction to guarantee the security from different aspects. Table 4 shows the market analysis and its strategy:

Table 3.Market analysis

	Market	**Suggested project**
Used Encryption Algorithm	TDES	TDES and DES-EC
Security level	Almost one security level	Three security levels
Acknowledgement message	Only after the transaction has been processed	Before and after the transaction process
Biometric scanners used	Fingerprint is commonly used	Fingerprint, iris and retina

The multimodal biometrics ATM presented in our proposal will be the first over world according to table 4 and our research.

Conclusion

This study provides a multi model identification system that combine three different biometrics, fingerprints, retinas and irises, which are considered as the most three accurate biometrics, with using PIN that is already used. By using different biometrics, the administrator can decide the required security level for each transaction, deposit/draft process for customers, Building

database of the three different biometrics templates used (Fingerprint, Iris and Retina).

Using a fast and secured encryption algorithm, DES-EC, It took 67 mili seconds to encrypt the data, 23 milli seconds to decrypt the data. A simple database simulation carrying the cipher text of the customer's data, which is secure since in order to be broken, requires the key which is the biometric image, as well as the complex algorithm implemented. Implementing the fingerprint, iris and retina scanners and integrating it with the encryption algorithm using java.

Generating variable keys extracted from the used biometrics images to encrypt the templates (the templates mean the data of each customer, i.e. his name and his account details). At the beginning, for each transaction, we use key for encryption so for any customer, we have different keys for every transaction he/she will do. Finally, we present a simple graphical user interface simulating the transaction process in an ATM.

Acknowledgements

First, I would like to acknowledge the financial support of my study at Ahram Canadian University. Also I would like to express my sincere thanks and gratitude to my supervisors. Finally, Special thanks to Prof. Dr. Mohammed Ismail, my main supervisor, for his help in my research to bring it up.

Corresponding Author:
Dr. Ghada Abdelhady
Department of Computer Networks
Faculty of computer science, Ahram Canadian University, 6th October city, Egypt.
E-mail: ghada.abdelhady10@gmail.com

References

1. Ghada Abdelmouez M., Fathy S. Helail, and Abdellatif A. Elkouny, "New DES based on Elliptic Curves", WASET - RIO DE JANEIRO 2010 Conference Program, march 2010.
2. William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, November 16, 2005.
3. Knudsen L.R., Block Ciphers- Analysis, Design and Applications, Ph.D. thesis, DAIMI PB-485, Aarhus University, Denamark, 1994.
4. Mao W. Modern Cryptography Theory and Practice, Prentice Hall PTR, July 25, 2003.
5. ChristofPaar · Jan Pelzl, "Understanding Cryptography ", A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010.
6. Torri N., K. Yokoyama, 'Elliptic Curve Cryptosystems', Fujtsu Sci. Tech. J. pp. 140-146 (December 2002).
7. Ghada Abdelmouez M., Fathy S. Helail, Abdellatif A. Elkouny, "DES Enhancement Using Elliptic Curve Equation", CNIR journal, May 2010.
8. Thomas Wollinger, Jorge Guajardo, and Christ of Paar, "Cryptography in Embedded Systems: An Overview", Department of Electrical Engineering and Information Sciences Communication Security Group (COSY), Ruhr-Universit ÄatBochum, Bochum, Germany, Proceedings of the Embedded World 2003 Exhibition and Conference, pp. 735-744, Design & Elektronik, Nuernberg, Germany, February 18-20, 2003.
9. Hagai Bar-El, "Security Implications of Hardware vs. Software Cryptographic Modules", White Paper, Discretix Technologies Ltd., Information Security Analyst, October 2002.
10. Sandro Bartolini, Paolo Bennati, Roberto Giorgi, Enrico Martinelli, "Elliptic Curve Cryptography support for ARM based Embedded systems", Dept. Ingegneria de ll' Informazione, University of Siena, Via Roma 56, 53100 Siena, Italy.
11. Avanindra Kumar Lal and SandipDutta, "ECC Based Biometric Encryption for Network Security", Journal of Computing, volume 3, issue 6, June 2011, issn 2151-9617.
12. Illiasaak Ahmad1, Norashikin M. Thamrin1, Mohamed Khalil Hani, "Crypto Embedded System for Electronic Document", Regional Postgraduate Conference on Engineering and Science (RPCES 2006), Johore, 26-27 July.

7/5/2014