MATEC Web of Conferences **42**, 06003 (2016)
DOI: 10.1051/matecconf/20164206003

Enhanced ATM Security using Biometric Authentication and Wavelet Based AES

Ajish Sreedharan[1]

[1]*Assistant professor, Department of Computer Science and Engineering, College of Engineering Perumon, Kollam, Kerala, India.*

Abstract. The traditional ATM terminal customer recognition systems rely only on bank cards, passwords and such identity verification methods are not perfect and functions are too single. Biometrics-based authentication offers several advantages over other authentication methods, there has been a significant surge in the use of biometrics for user authentication in recent years. This paper presents a highly secured ATM banking system using biometric authentication and wavelet based Advanced Encryption Standard (AES) algorithm. Two levels of security are provided in this proposed design. Firstly we consider the security level at the client side by providing biometric authentication scheme along with a password of 4-digit long. Biometric authentication is achieved by considering the fingerprint image of the client. Secondly we ensure a secured communication link between the client machine to the bank server using an optimized energy efficient and wavelet based AES processor. The fingerprint image is the data for encryption process and 4-digit long password is the symmetric key for the encryption process. The performance of ATM machine depends on ultra-high-speed encryption, very low power consumption, and algorithmic integrity. To get a low power consuming and ultra-high speed encryption at the ATM machine, an optimized and wavelet based AES algorithm is proposed. In this system biometric and cryptography techniques are used together for personal identity authentication to improve the security level. The design of the wavelet based AES processor is simulated and the design of the energy efficient AES processor is simulated in Quartus-II software. Simulation results ensure its proper functionality. A comparison among other research works proves its superiority.

1 Introduction

Nowadays security becomes a great issue in every part of life. Passing of information faces massive problems due to various types of attacks to the communication link. Many security algorithms are available to protect information from being hacked. The biometric authentication[1] process adds a new dimension of security for any person sensitive to authentication. Biometric based authentication offers several advantages over other authentication. Fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. Biometrics is a rapidly advancing field that is concerned with identifying a person based on his physiological or behavioral characteristics.

As the Automated Teller Machines (ATM)[2] technology is advancing, fraudsters are devising different skills to beat the security of ATM operations. Various forms of fraud are perpetuated, ranging from ATM card theft, skimming, pin theft, card reader techniques, pin pad techniques, force withdrawals and lot more. Managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences. Considering the numerous security challenges encountered by Automated Teller Machines[2] and users and given that the existing security in the ATM system has not been able to address these challenges, there is need to enhance the ATM security system to overcome these challenges.

This paper presents a secured, ultra-high speed and energy efficient ATM banking system that is highly secured system compared with the existing one. At present most of the ATM systems use triple data Encryption Standard (3DES)[3]. Which has some drawbacks; such as it is vulnerable to differential attacks and also slow in performance. This paper presents security in two ways in which both the fingerprint image for the client side security and the AES algorithm for the secured communication in between. Based on these perspectives, Advanced Encryption Standard[3] was accepted as a FIPS[4] standard in November 2001, after which AES became the most popular encryption standard all over the world.

A lot of researchers are working to improve the speed of AES[3] as well as the other aspects like area, latency, power etc. To make the AES faster and securer, some researchers introduced hardware realizations and S-box optimizations. Today most of the researchers involving the execution of the Advanced Encryption Standard[3] algorithm are fallen into three areas: ultra-high speed encryption, very low power consumption, and algorithmic integrity. Many research works have been done by different hardware realizations using ASIC and FPGA[4] technology.

Article available at http://www.matec-conferences.org or http://dx.doi.org/10.1051/matecconf/20164206003

In this paper, a new AES[3] algorithm for image encryption algorithm is proposed which is based on wavelet transform[5] and energy efficient S-box[4]. First of all, wavelet decomposition is used for concentrating original image in low-frequency wavelet coefficients [6], then low power AES is applied to encrypt the low-frequency wavelet coefficients. Secondly, an XOR operation is used for high-frequency wavelet coefficients and the encrypted low-frequency wavelet coefficients (as a key stream), so that the image information contained in high-frequency wavelet coefficients is hidden; then a wavelet reconstruction is used for spreading the encrypted low-frequency part to the whole image.

2 Research Background

ATM[2], the abbreviation of "Automated Teller Machine" allows the account holder to have transactions with their own accounts without the opportunity to access the entire bank's database. The idea of self-service in retail banking was developed through independent and simultaneous efforts in Japan, Sweden, the United Kingdom and the United States. In the USA, Luther George Simjian[7] has been credited with developing and building the first cash dispenser machine. The first cash dispensing device was used in Tokyo in 1966.

Figure 1. A Conventional ATM System

ATM first came into use in December 1972 in the UK. Figure 1 shows a conventional ATM system. IBM 2984 was designed for request of Lloyds Bank[7]. ATM is typically connected directly to their hosts or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. For transaction security, all communication traffic between ATM and transaction process is encrypted by cryptography. Nowadays most of ATM use a Microsoft OS primarily Windows XP Professional or Windows XP Embedded or Linux.

2.1 Fingerprint

Fingerprint is a characteristic unique for each person which contains unique identifiable piece of information. The uniqueness in each fingerprint is due to the peculiar genetic code of DNA[8] in each person. Ridges and valleys are the parts of fingerprint that provide friction for the skin. The direction and location of ridges[8] make the identification. A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human.

2.2 AES Algorithm

The Rijndael[3] algorithm referred to as the AES Algorithm[3], is a symmetric key block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Figure 2 shows that AES has four stages required for every round except that the last round excludes the mix column phase and the first round has only key addition. The four stages of Rijndael algorithm (AES algorithm)[3] are:

Substitute Bytes: This function uses an S-box to perform a byte-by-byte substitution of the block. For encryption and decryption, this function is indicated by SubBytes() and InvSubBytes() [3] respectively.

Shift Rows: This is a simple permutation. For encryption and decryption, this function is indicated by ShiftRows() and InvShiftRows() [3] respectively.

Mix Columns: This is a substitution that makes use of arithmetic over GF (2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. For encryption and decryption, this function is indicated by MixColumns() and InvMixColumns() [3] respectively

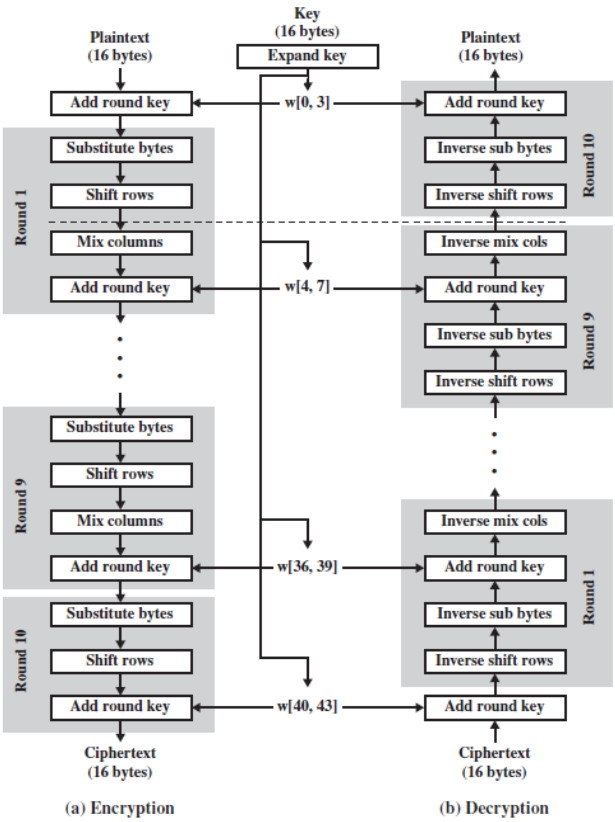


Figure 2. AES Encryption and Decryption.

Add Round Key: This function does a bitwise XOR oper- ation of the current block with a portion of the expanded key. For both encryption and decryption this function is indicated by AddRoundKey(). For the AddRoundKey() [3] the inverse is achieved by XORing

the same round key to the block, using the result: A ⊕ A ⊕ B = B.

3. Design of Biometric Authentication and Wavelet Based AES

In this section, the design consideration of proposed ATM system is presented to achieve highly secured ultra-high speed and low power consumed ATM system. Two basic designs considered throughout this paper are biometric authentication (fingerprint) and cryptography (AES).

3.1 Fingerprint Design

The fingerprint of client taken with a image capturing device is processed over a numerous steps to get hexadecimal data. Some considerations are taken to achieve higher security for this ATM.

Original Image: The image is acquired using capturing device inside of which contains a sensor and a LED[8], continuously light. When an object is pressed on the image capturing portion the light intensity becomes high and the sensor senses the situation and deliveries the signal to CPU instructs the device to capture image.

Threshold Image: Threshold[8] condition is the simplest method of image segmentation. This process executes every pixel of the image and only counts those pixels for threshold in which pixel is more than 129. The simplest segmentation method separates out regions of an image corresponding to objects which we want to analyze. This separation is based on the variation of intensity between the object pixels and the background pixels. This threshold operation can be expressed as: (The image is an array) in Equation 1.

$$dst(x,y) = \begin{cases} maxval & \text{if } src(x,y) > threshold \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Figure 3 shows that the original image is converted to hex values by the processes. After the threshold process, the threshold image is found whose data is provided in Figure 3.

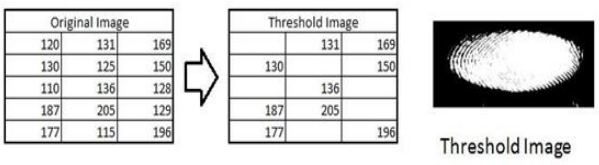


Figure 3. Threshold Process and Image

Rotate & Cropped: Align the major axis parallel with X axis taking only the fingertip part of the image. The image in elliptical shape, has a major and minor axis. To process the image properly, the image's major axis should be on X axis. To create the position, the major axis as X axis, at first counts the value of angle difference between the image's major axis and X axis then rotates the major axis reversed as the value of angle difference.

Figure 4 illustrates the final image that being rotated and cropped. To extract a rectangular portion of an image, the in crop function is utilized. Finally the image will be specific at position and portion for use.

Figure 4. Rotated and Cropped Image

Edge of Ridge: This is the last step. For Canny algorithm[8], the object finds edges by looking for the local maxima of the gradient of the input image. The calculation derives the gradient using a Gaussian filter[8]. Any pixel connected to a strong edge and having a magnitude greater than the low threshold corresponds to a weak edge. The Canny block computes the automatic threshold values using an approximation of the number of weak and non-edge image pixels. Figure 5 illustrates the edge of ridge at the final stage. Using this approximation for the estimated percentage of weak edge and non-edge pixel (used to automatically calculate threshold values) parameters, this algorithm performs more robust to noise and more likely to detect true weak edges.

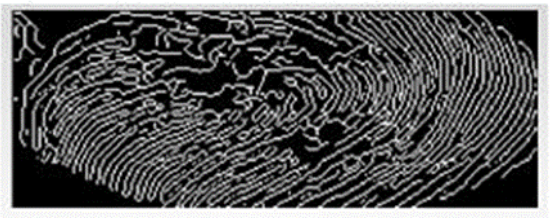


Figure 5. Edge of Ridges

3.2 Haar Discrete Wavelet Transforms

The frequency domain transform applied in this algorithm is Haar-DWT [6], the simplest DWT. A 2-dimensional Haar-DWT [6] consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 6.

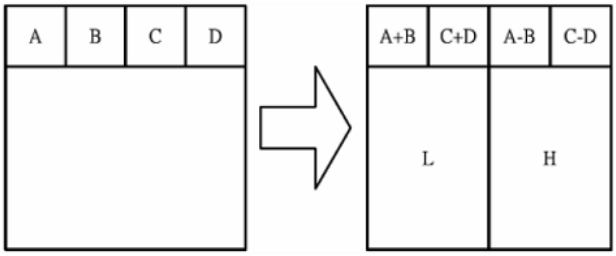


Figure 6. The horizontal operation on the first row.

Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the

high frequency part of the original image (denoted as symbol H).

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 7. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

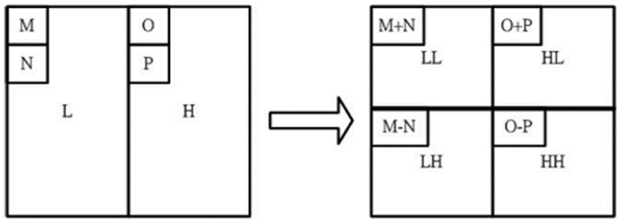
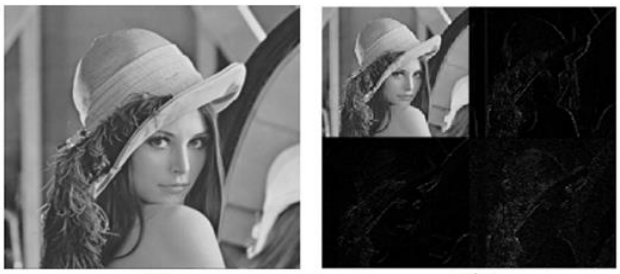


Figure 7. The vertical operation

The whole procedure described above is called the first-order 2-D Haar-DWT[6]. The first-order 2-D Haar-DWT applied on the image "Lena" is illustrated in Figure 8.



(a) (b)

Figure 8. (a)Original image-Lena, (b) Result after the first-order 2-D Haar-DWT

3.3 Wavelet Based AES

In this paper, a new image encryption algorithm is proposed which is based on wavelet transform low power S-box based AES algorithm. First of all, wavelet decomposition is used for concentrating original image in low-frequency wavelet coefficients [9], then low power S-Box based AES algorithm is applied to encrypt the low-frequency wavelet coefficients. Secondly, an XOR operation is used for high-frequency wavelet coefficients and the encrypted low-frequency wavelet coefficients (as a key stream), so that the image information contained in high-frequency wavelet coefficients is hidden; thirdly, a wavelet reconstruction is used for spreading the encrypted low-frequency part to the whole image.

3.4 Low Power Design of AES Processor

To get low power AES processor, the overall power consumption of the ATM system, the S-box implementation in Galios Field $(2^4)^2$[10] instead of GF (2^8) has been proposed. S-box is the most costly transformation in AES, on the aspect of both time and area. Rijme[10] suggested an alternative approach to calculate multiplicative inverses in S-Box. Since then, the relevant research has proved that the composite field $GF(2^4)^2$ based arithmetic provides the least gate count and the shortest critical path to calculate multiplicative inverse of a byte, which is the key step in S-Box. This conversion involves an isomorphic map function before and after inversion in each round. In this design it takes 128-bit key for the AES processor. Therefore it needs ten map functions for each block (128-bit) from finite field to composite field and ten inverse map functions for encryption. In addition, the key generator having S-Box includes another ten mapping and ten inverse mapping.

To save the overhead caused by mapping, this design converts the whole AES algorithm from GF(2^8) to $GF(2^4)^2$, which needs only one forward mapping before the initial round and one backward mapping after the final round. Beside this only one forward mapping is needed for the key schedule.

4. Proposed System

The proposed system consists of a fingerprint-capturing device, which captures image of the client. Taken image is fed to the image-processing device within the ATM machine. The processed image is converted to 1024 bit of

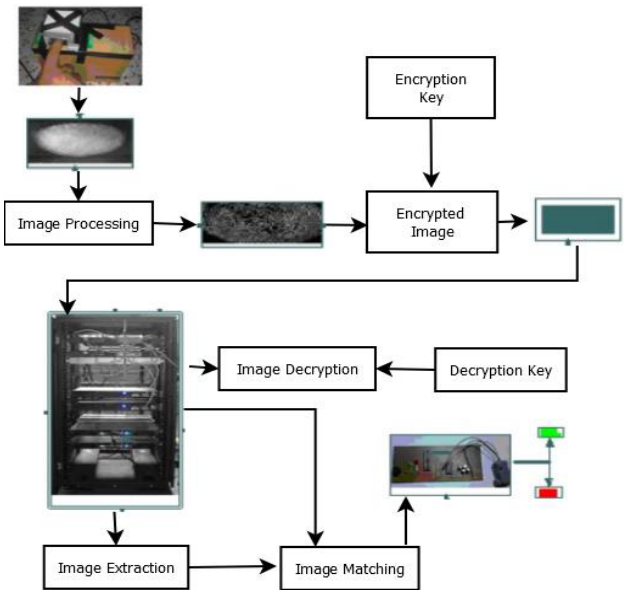


Figure 9. Proposed ATM Design

binary data which is the input data of the AES processor encrypting the data with the help of 4 digit decimal key that is provided by the user as password. The data is encrypted using wavelet based low power AES and passed to the bank server through a communication link. At the bank side, the received cipher message is decrypted with the help of same key. The original image is reproduced at this step. Then the decrypted image of fingerprint is matched with the previously stored image of the authentic customer for the specific request of the client. If the request is valid then an acknowledgement message is sent to the ATM machine through the same communication link. If the acknowledgement is "Yes"

the client can withdraw money from the ATM machine. If acknowledgement is "No" an error message is shown the screen of the ATM machine. In this paper the acknowledgement device which switches on a green light if the acknowledgement is "Yes" otherwise it turns on a red light. Figure 9 shows the proposed ATM system.

5. Performance

The proposed system is one of the most secured and least energy consumed systems compared to the existing ATM systems. There are two reasons; firstly acquisition device captures image accurately. The error of the device is negligible. Secondly using AES makes the system more secured, fast and energy efficient. The fingerprint image is processed to get the hexadecimal number values which are discussed earlier in the Section 'design consideration'. The values that come out from image processing section are the input data of the AES processor.

Dynamic power consumed by the encryption process is compared to the other related work in Table 1 and found the superiority over other research works.

Table 1. Comparison with other related works

Design	Device	Static Power (mW)	Dynamic power (mW)
Alam	Virtex II	80	821
Xinmiao Zhang	Virtex 4	80	125
Kenny D	Cyclone II	80.03	192.34
This work	Cyclone II	80.09	93.90

The Wavelet Based AES image encryption algorithm is tested and evaluated based on software and hardware simulation. Different standard images have been used "lena" "cheetah" and Baboon (greyscale format) in the simulations which are encrypted with wavelet Based AES and AES algorithms. Table II shows the average time required by Wavelet Based AES and AES for each image. From the Table it is clear that Wavelet Based AES algorithm is much faster than AES algorithm.

Table 2. Average Time Required by AES and Wavelet AES for Different Images

Image(Size)	AES Encryption Time	Wavelet Based AES Encryption Time
Lena(256*256)	31.75 ms	8.2 ms
Cheetah(200*320)	29.25 ms	7.52 ms
Baboon(512*512)	127.99 ms	31.99 ms

6. Conclusion

Biometric authentication scheme for ATM banking system using energy efficient and wavelet based AES processor is presented in this paper. A number of novel design considerations have been taken in designing the ATM system. It is capable safeguard against all known attacks. The whole system is simulated in Quartus-II software. The simulation result shows the proper functionality of the system. The hardware implementation also carried out by implementing the LED based signaling. The encrypted message is sent to the server and compared with the stored fingerprint image. If the decrypted image and stored image is matched together, then a green LED turns on, otherwise a red LED is alight. The hardware also shows the proper functionality of the system. This design is also compared with the other research work.

References

1. Vaclav Matyas and Zdenek Rha "Biometric Authentication Security and Usability", 3rd ed. IEEE.
2. Selina Oko and Jane Oruh "Enhanced ATM Security System using Biometrics", 3rd ed.International Journal of Computer Science Issues, Vol. 9, Issue 5, No **3**, September (2012) ISSN (Online): 1694-0814.
3. William Stallings, "Cryptography and Network Security Principles and Practice", Prentice Hall.
4. D. Kenny "Energy Efficiency Analysis and implementation of AES on an FPGA", Waterloo, Ontario, Canada, (2008).
5. Shuo Zhang, Ruhua Cai and Yingchun Jiang," An Image Encryption Algorithm Based on Multiple Chaos and Wavelet Transform", (2009) IEEE pp. 178-188.
6. Po-Yueh Chen and Hung Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering.
7. Fumiko Hayashi, Richard Sullivan, and Stuart Weiner " A Guide to the ATM and Debit Card Industry Payments System" Research Department Federal Reserve Bank of Kansa City, Kansas City, Missouri, USA (2003).
8. Le Hoang Thai and Ha Nhat Tam "Fingerprint recognition using standardized fingerprint model " IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No **7**, May (2010).
9. Long Bao, Yicong Zhou, and C. L. Philip Chen, "Image Encryption in the Wavelet Domain", Mobile Multimedia/Image Processing, Security, and Applications (2013).
10. J. V. Dyken and J. G. Delgado-Frias. "FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm" School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164-2752, USA, Available online 16 December (2009)