Des Enabled Fingerprint System

Gobinath Subramaniam, Kalyani Subramanian, Senthil Raja Balakrishnan,
Baskaran Kaliaperumal
Government College of Technology, Coimbatore
Tamil Nadu, India

***Abstract* - Biometrics systems function to identify individuals by matching a specific personal characteristic, the biometrics identifier, with one previously recorded. Biometric identification considers individual physiological characteristics and/or typical behavioural patterns of a person to validate their authenticity. Fingerprints are used to generate the key; this key value is used in the Data Encryption Standard (DES) algorithm. Initially the finger print image is converted into a pixel matrix. After the matrix conversion the matrix is applied into the one way hash function. The hash code value is a 64 bit string value. This hash code value is passed into the DES algorithm as key for the encoding and decoding process. This 64-bit key value is converted as a 56 bit key value by the DES algorithm computational operations. The system also performs an authentication checking process in the decryption process to verify the correctness of the key value. Fingerprint Selection contains receiving finger print data and conversion of finger print values into matrix tasks. This accepts the finger print data as an image file. Key Generation generates the key for the security system. Using the selected finger print image data generates the key value. Encryption performs the document encoding task. The user can select any file for the encryption process. Decryption process is performed to retrieve the original document from the encoded document. Biometrics offers new perspectives in high-security applications while supporting natural, user-friendly and fast authentication.**

Keywords* - *Data Encryption Standard, Authentication, Key Generation

I. Introduction

Biometrics offers new perspectives in high-security applications while supporting natural, user-friendly and fast authentication [1]. Biometric identification considers individual physiological a person to validate their authenticity [3]. Compared to establish methods of person identification, employing PIN-codes, passwords, magnet- or smart cards, biometric characteristics offer the following advantages:

- They are significant for each individual,
- They are always available,
- They cannot be transferred to another person,
- They cannot be forgotten or stolen,
- They always vary 1.

General biometrics systems consist of the five sub-systems data collection, transmission, signal processing, storage, and decisions.

The term BIOMETRICS has come to be associated with the automatic identification of a person based on a feature or characteristic. These may be based on either:

- A physiological characteristic such as a fingerprint or face
- A behavioural characteristic such as a signature or voice

A variety of methods and techniques are available today, with the most common being:

Iris/Retina, Voice, Signature, Fingerprint and Face.

Generally, face, signature and voice are considered to be a lower level of security than fingerprint and iris, with iris scanning being the method of choice for extremely sensitive areas. This does not mean that the others aren't effective, but there is a price difference between the high and low end. It is a good idea to select a system that meets the basic needs [2].

Biometric systems are not perfect. An authorized user may be rejected by the system while an unauthorized user may gain access to it. Lighting, climate conditions low quality equipment or inexperience usually causes the False Rejection Rate (FRR). The False Acceptance Rate (FAR) is caused by the security standard being too low. The later is far more serious, as it poses a great risk to have unauthorized people gaining access to the systems. The FARs and FRRs vary between biometric techniques, but iris scanning has proven to be the only one that has never had a false acceptation

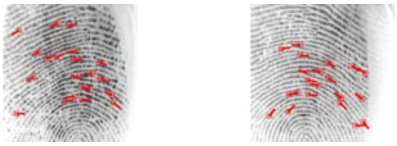


Fig. 1. Two different fingerprint images of one user.

Biometric systems are becoming commonplace in the society. Though many people have failed to accept these new methods of identification/verification because of the "Big Brother" fear, education and first-hand experience with the technology is slowly winning some people over. One thing to remember is that even though biometrics are a very strong method of security, a single "key" should not suffice. It is generally considered that the use of 2 biometrics or the combination of a biometric with a more traditional method can ensure a higher standard of security [3].

II. RELATED WORK

A. *An Automatic Identity Authentication*

An Identity Authentication System Using Fingerprints submitted by Anil Jain, Lin Hong, Sharath pankanti and Ruud Bolle at Department of Computer Science Michigan State University.

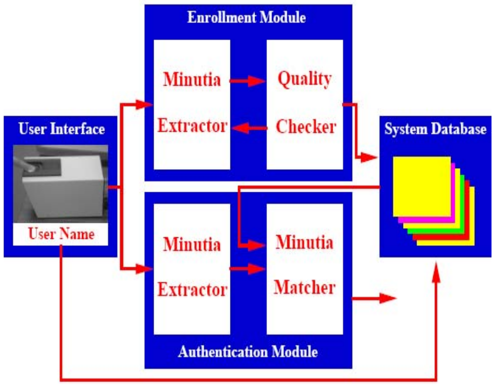


Fig. 2. Architecture of Automatic Identity Authentication

To introduce a prototype automatic identity authentication system is capable of automatically authenticating the identity of an individual using fingerprints. The architecture of the automatic identity authentication system is shown in Figure. It consists of four components: user interface, system database, enrollment module, and authentication module. The task of enrollment module is to enroll persons and their fingerprints into the system database. If a fingerprint image is of poor quality, it is enhanced to improve the clarity of ridge/valley structures and mask out all the regions that cannot be reliably recovered.

The enhanced fingerprint image is fed to the minutiae extractor again. Because the current quality checking algorithm is very slow, it is only used in the enrollment module. The task of authentication module is to authenticate the identity of the person who intends to access the system. The person to be authenticated indicates his/her identity and places his/her finger on the fingerprint scanner; a digital image of his/her fingerprint is captured and minutiae pattern is extracted from the captured fingerprint image and fed to a matching algorithm which matches it against the person’s minutiae templates stored in the system database to establish the identity.

III. MATERIALS AND METHODS

Fingerprints are used to generate the key. This key value is used in the DES algorithm. The system also performs an authentication checking process in the decryption process to verify the correctness of the key value. The system is designed to secure any type of file. The design of the system consists four phases. They are the finger print selection, key generation, document encoding and document decoding [7]. The software portion entitled as ‘‘BIOMETRIC BASED SECURITY SYSTEM’’.

A. *Finger Print Selection*

This section contains receiving finger print data and conversion of finger print values into matrix tasks. There are different methods are used to collect the finger print image data. Using the finger print scanner or the Image scanning devices captures finger print data. The user can also feed the fingerprints data from a stored image file.

The scanned image file data is converted as a pixel matrix. In this process the compressed image is decompressed. After the decompression process the system returns a pixel matrix. The size of the pixel matrix is derived from the height and width of the finger print image.

B. *Key Generation*

This section generates the key for the security system [3]. Using the selected finger print image data generates the key value. Initially the finger print image is converted into a pixel matrix. After the matrix conversion the matrix is applied into the one way hash function. The hash code value is a 64 bit string value. This hash code value is passed into the DES algorithm as key for the encoding and decoding process. This 64-bit key value is converted as a 56 bit key value by the DES algorithm computational operations.

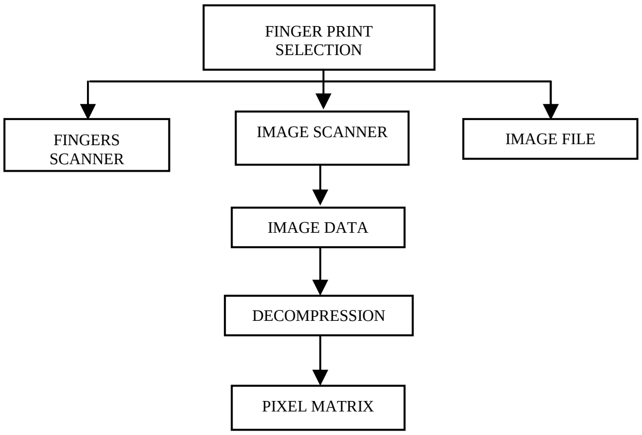


Fig. 3 Finger Print Selection Process

C. Encryption

This section performs the document encoding task. The user can select any file for the encryption process. Using the generated key value performs the encryption process. It is very important that the user must generate the key value before performing the encryption or decryption task. The encrypted data is stored into a file selected by the user. The system also displays the progress of the encoding process [6].

The input file and output file sizes are displayed by the system. The output file is saved as an encoded format file. It is not possible to read the content of the encoded file without the performing the decoding task. The DES algorithm is used for the encoding process. The input file applied into the encoding process as blocks. All the encoded blocks are stored as an output file. The system also includes an encoded authentication key. This key value is used to verify the authentication for the decryption process. This authentication process is internally handled by the system itself.

D. Decryption

Using this section does the decoding process. The decoding process is performed to retrieve the original document from the encoded document. The DES algorithm is used for the decoding process. Two main tasks are performed in the unlock process. They are decoding and the key authentication process. At first the key authentication process is performed. The decoding process is done only the user produces an authenticated key value. If the produced key is not an authorized one then the process will be automatically terminated by the system.

The user selects the encoded file name and the output file names. The decoding process progress is displayed by the system. After completing the decoding process the system displays a message the decoded content is stored as file. After the decoding process, the user can get the original file without any change. The same key must be used for the encoding and the decoding process.

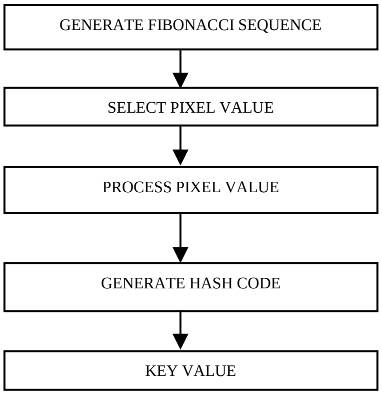


Fig. 4 Key Generation Process

E. Obtaining & Processing Fingerprint Data

Every fingerprint can be broken down into two basic features, called ridges and valleys [4]. By examining these characteristics, it is possible to extract data from raw fingerprints and store it in a computer database for future comparisons. Images can be captured using one of several devices, including:

- Optical Scanners
- Thermal Scanners
- Capacitive (Solid-State) Scanners

There are currently two accepted methods for extracting this data: minutia-based and correlation-based. Minutia-based is the more microscopic of the two, locating ridge branches and endings and assigning them and XY-coordinate that is then stored in a file. Correlation-based looks into the overall pattern of ridges and valleys. Instead of looking for tiny minutia points, the locations of whorls, loops and arches and the directions that they flow in are extracted and stored. On the other hand, correlation-based comparisons can be affected by image translation and rotation.

After the initial setup of an authorized user, every time he or she wants to access the system, the fingerprint is run through the same algorithms used when it was stored. This data set is compared to the original data set on file, and then it is either accepted or rejected. Most authentication systems grapple with this False Rejection Rate/False Acception Rate (FRR/FAR). Simply put, authorized users shouldn't be rejected and unauthorized users shouldn't be accepted. No system has been created that is 100% accurate.

IV. Implementation

A. DES Core Function

Once the key scheduling and plaintext preparation have been completed, the actual encryption or decryption is performed by the main DES algorithm. The 64-bit block of input data is first split into two halves, L and R. L is the left-most 32 bits, and R is the right-most 32 bits. The following process is repeated 16 times, making up the 16 rounds of standard DES. We call the 16 sets of halves L[0]-L[15] and R[0]-R[15].

i. R[I-1] - where I is the round number, starting at i - is taken and fed into the E-Bit Selection Table, which is like a permutation, except that some of the bits are used more than once. This expands the number R[I-1] from 32 to 48 bits to prepare for the next step.

ii.The 48-bit R[I-1] is XORed with K[I] and stored in a temporary buffer so that R[I-1] is not modified.

iii. The result from the previous step is now split into 8 segments of 6 bits each. The left-most 6 bits are B[1], and the right-most 6 bits are B[8]. These blocks form the index into the S-boxes, which are used in the next step. The Substitution boxes, known as S-boxes, are a set of 8 two-dimensional arrays, each with 4 rows and 16 columns. The numbers in the boxes are always 4 bits in length, so their values range from 0-15. The S-boxes are numbered S[1]-S[8].

iv. Starting with B[1], the first and last bits of the 6-bit block are taken and used as an index into the row number of S[1], which can range from 0 to 3, and the middle four bits are used as an index into the column number, which can range from 0 to 15. The number from this position in the S-box is retrieved and stored away. This is repeated with B[2] and S[2], B[3] and S[3], and the others up to B[8] and S[8]. At this point, you now have 8 4-bit numbers, which when strung together one after the other in the order of retrieval, give a 32-bit result.

v. The result from the previous stage is now passed into the P Permutation.

vi. This number is now XORed with L[I-1], and moved into R[I]. R[I-1] is moved into L[I].

vii. At this point we have a new L[I] and R[I]. Here, we increment I and repeat the core function until I = 17, which means that 16 rounds have been executed and keys K[1]-K[16] have all been used.

When L[16] and R[16] have been obtained, they are joined back together in the same fashion they were split apart (L[16] is the left-hand half, R[16] is the right-hand half), then the two halves are swapped, R[16] becomes the left-most 32 bits and L[16] becomes the right-most 32 bits of the pre-output block and the resultant 64-bit number is called the pre-output.

V. Results And Analysis

The system produces intermediate results. Encoded documents are applied into the decoding process with the same key and also the module is tested with different finger print values. The testing results show that the system is a reliable one. The system provides a high level security for the documents and also for the key. The decoding process results show that the system returns the original content of the encoded file without any loss.

A. Analysis

The system is tested with different number of inputs. The results of this system are analyzed with the consideration of the following factors. They are time, file type and size, instant key generation process, security and authentication.

B. Process

The duration for the encryption and decryption process are measured and compared. The encryption and the decryption tasks take the same amount of time. The key generation time is very negligible one. The time that can be taken for the encryption and the decryption process is depends upon the input file size. If the file size is increased then the process time is also increased. The key generation time is almost same for any finger print image. The hardware configuration may affect the execution time [5].

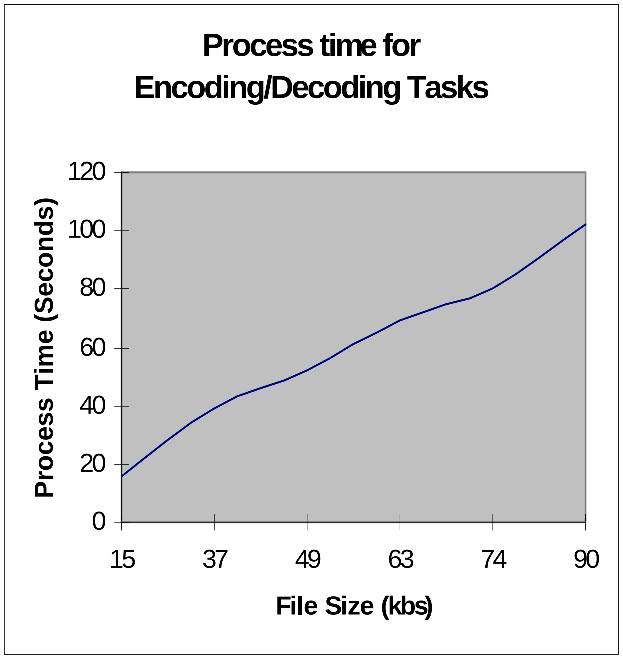


Fig. 5 Process Time for the Tasks

C. Security

The system does not require keeping the key value for future process. The key is generated before each and every encoding and decoding process. In this system it is impossible to miss the key value. The encoding process ensures the document security.

D. Authentication

The system uses a different authentication procedure to verify the authenticity of the key value. This authentication task is handled by the system itself. The system does not require any user action for the key authentication process.

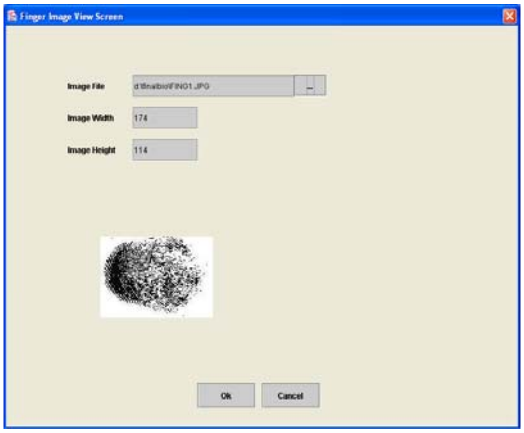
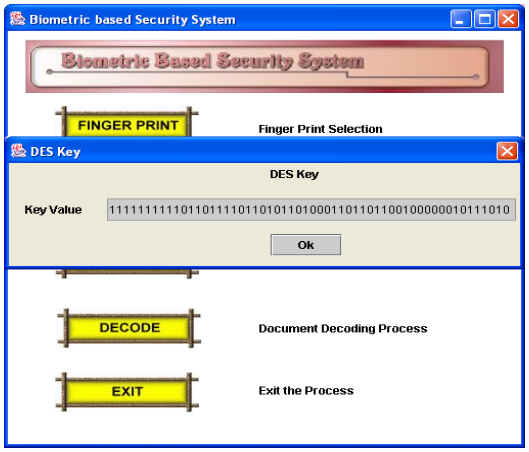

Finger Image View Screen

Image File d:\finalbio\FING1.JPG

Image Width 174

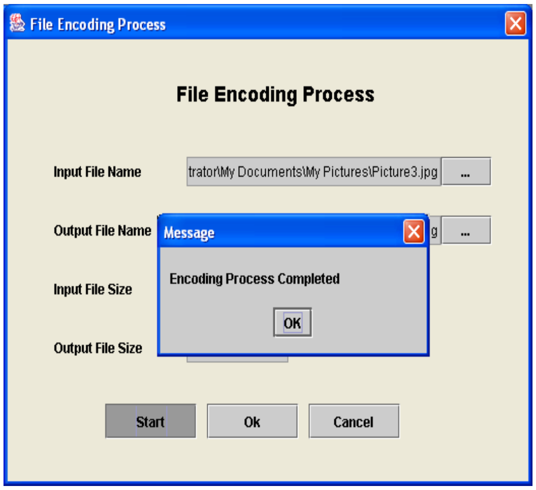
Image Height 114

Fig. 6 Finger Print Selection


Biometric based Security System
Biometric Based Security System
FINGER PRINT
Finger Print Selection
DES Key
DES Key
Key Value
Ok
DECODE
Document Decoding Process
EXIT
Exit the Process

Key Value 11111111110110111101101011010001101101100100000010111010

Fig. 7 Key Generation


File Encoding Process

File Encoding Process

Input File Name trator\My Documents\My Pictures\Picture3.jpg

Output File Name

Input File Size

Output File Size

Message

Encoding Process Completed

Fig. 8 Completion of Encoding

VI. Conclusion

This system is developed to provide security for the files. The system uses the biometrics technology for the security providing medium. Generally passwords and smart cards are used for the security systems. This system uses the fingerprints for the security system. Password can be hacked by trial and error basis. But it is not possible to break the biometric based security system. The system uses two algorithms for the process. The one way hash function is used for the key build process and the DES algorithm is used for the encryption/decryption process. The system is tested with various samples and the performance of the system is very good. The system is tested with different type of fingerprint image formats.

References

[1] Martín Abadi , Andrew D. Gordon,‘‘A calculus for cryptographic protocols: the spi calculus”, Conference on Computer and Communications Security, Proceedings of the 4th ACM conference on Computer and communications security, Pages: 36 – 47, 1997.

[2] A.Eskicioglu, L.Litwin., “Cryptography”, IEEE Transactions on Security & Privacy, Volume 20, Issue 1, Feb/Mar 2001 Page(s):36 – 38.

[3] R.Sanchez-Reillo, C.Sanchez-Avila, A.Gonzalez-Marcos, “Biometric identification through hand geometry measurements”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 22, Issue 10, Oct 2000 Page(s): 1168 – 1171.

[4] Bruce Schneier, “Applied Cryptography Protocols, Algorithms” Wiley Publication, 2nd Edition.

[5] Naughton.P and H.Schildt, “Java 2: The Complete Reference”, McGraw-Hill, 1999.

[6] William Stallings, “Cryptography and Network Security Principles and practice”, Prentice Hall, Upper Saddle River, 2nd Edition.

[7] James L. Wayman, “Biometrics Identification”, Communications of the ACM, February 2000.