European Scientific Journal October 2013 edition vol.9, No.30 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431

CRYPTOSYSTEM FROM MULTIPLE BIOMETRIC MODALITIES

Haitham Wahdan, Eng.
College of Engineering and Technology, Arab Academy for Science, Technology & Maritime Transport, Cairo, Egypt
Abdel-Moneim Wahdan, Prof. Dr.
Faculty of Engineering, Ain Shams University, Cairo, Egypt
Aliaa A. A. Youssif, Prof. Dr.
Faculty of Computer and Information, Helwan University, Cairo, Egypt

Abstract

One of the most important parts of cryptographic systems is key generation. Researchers, for a long time period, have been inventing ways to produce tough and repeatable cryptographic keys. Keys that had these features are hard to be memorized and may be stolen or lost. For this purpose using biometric features to generate cryptographic key is the best way. Most previous Researchers focused to extract features and generate key from an individual biometric, but it is hard to be used in multi stages cryptographic systems. Therefore, this approach is enhancing the cryptographic systems by using long and complex cryptographic keys that are hard to be guessed and do not need to be memorized and provide better usage in multi stages cryptographic systems by extracting features from multi biometrics, That provides accuracy 99.83% with time less than using individual biometric by 90%.

Keywords: Biometrics, Cryptosystem, ECC, DCT, DWT

Introduction

In the growing of increased demand of security and fast progression in communication, networking, computer software's and mobility, there are huge demand in better user authentication techniques. Many of the authentication systems are not very reliable (can be broken, stolen or forgotten), furthermore the attackers can control access to secured locations for passwords. For these problems, one of the most effective ways is using biometrics (iris, fingerprint, voice, face, DNA …) to prevent stolen or forgotten (Srivastava, Agrawal, Mishra, Ojha and Garg 2013). In this paper one of the newest approaches in cryptography is combining the human

biometrics with cryptographic systems. This approach does not need to store any template in database. This will minimize attacking risks and preventing any threats can happen on DB level.

This paper uses error correction code instead of storing template to make sure that the keys extracted from biometrics are correct. This is also an authentication technique, so the person who has the correct parities and also the correct biometrics able to decrypt the encrypted message.

Literature Overview

This part presents an overview on biometrics, cryptosystem and error correction code.

Biometrics & Biometric System

The identification of Biometric is "something that you are", or "something that you do". It differentiates between the authorized person and intruders (Tico, 2001). Biometrics is divided into two major parts physiological and behavioral characteristics and their types as shown in figure1.

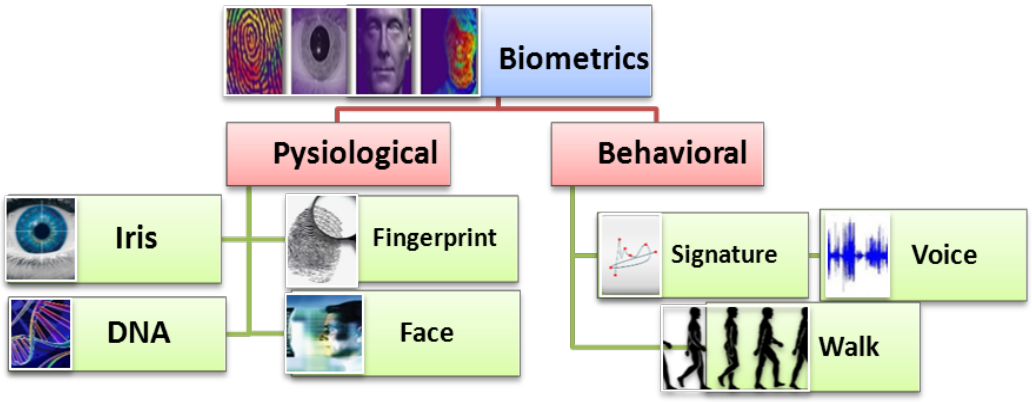

Figure 1: Classifications of biometrics.

There are many ways to extract feature from biometrics, for example in voice using Mel-frequency cepstral coefficients (MFCCs), Wavelet, Spectral subtraction and Cepstrum Analysis (Gaikwad, Gawali and Yannawar 2010). Eyes, nostrils and mouth localization (prominent characteristics on the faces) are essential in face images (Hao, Anderson and Daugman 2006). There are also algorithms to extract an accurate and robust feature from face such as cosine transformation DCT (Shaojun 2009). The iris is an annular part between the pupil (inner boundary) and the sclera (outer boundary), which can approximately be taken as circles. One of the most powerful ways to extract feature is wavelet transform. It is a very

powerful tool for texture discrimination and a linear operation that decomposes a signal into components that appear at different scales (Seung, Kwanghyuk, Yeunggyu, and Jaihie 2003).

Cryptosystem

Cryptography is where security engineering and mathematics joining together (Anderson, Wiley, and Sons 2010). It is the practice and study of hiding information. Cryptosystem is the combination of three elements: an encryption engine, keying information, and operational procedures for their secure use. There are three main types of cryptography symmetric, asymmetric and one-way cryptography (Hash) shown in figure 2.

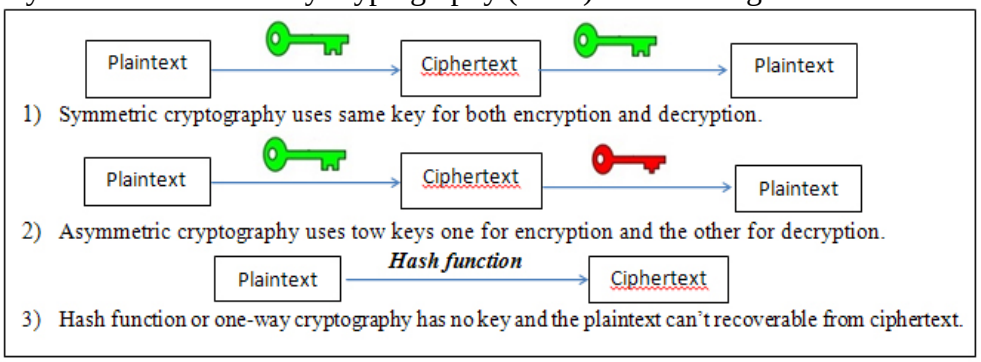

Figure 2: Cryptosystem types

Data Encryption Standard (DES)

The DES algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key but use 56 bit only and the remaining 8 bits are for error checks (Anderson, Wiley, and Sons 2010).

Error detection & correction

Even without malicious intervention, ensuring correct data is a difficult problem. Data that collected from biometrics is not identical may one or more bits can be flipped. This effect has always been present, but its effects have heightened as technology increased and key length increased (Dhotre and Baga, 2008).

Error detection means to decide whether the received data is correct or not without having a copy of the original message. Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.

Error Correction is a way to represent a set of symbols so that if any bit of the representation is flipped, you can still tell which bit it was. There

are two main classifications of errors single and burst error shown in figure 3.

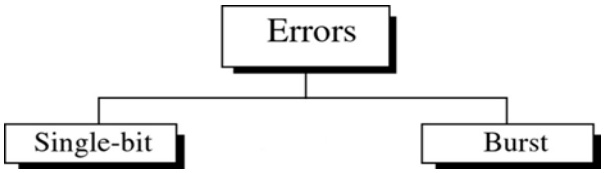

Figure 3: Error types.

Single bit error (Dhotre and Baga, 2008) means that only single bit was flipped it is least likely type of errors in serial data transmission because the noise must have a very short duration which is very rare; however this type of errors can be happen in parallel transmission shown in figure 4.

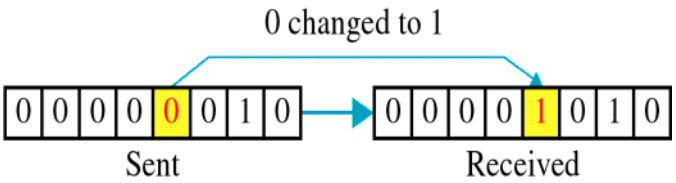

Figure 4: Single bit error.

Burst error (Dhotre and Baga, 2008) means that two or more bits in the data unit have changed. The errors do not necessarily occur in consecutive bits. The first corrupted bit to the last corrupted bit is the length of the burst. It may contain some bits in between are not corrupted shown in figure 5.

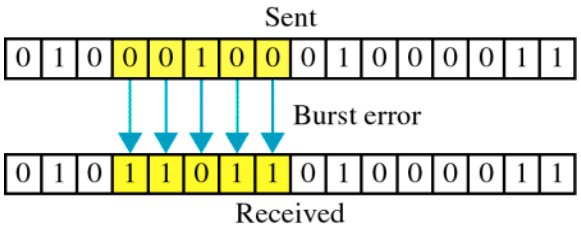

Figure 5: Burst error.

The main problem of biometrics is they are not identical every time you extract feature from them. The majority of the features are identical but there are some features will be different each time taking sample. For this reason using (ECC) Error Correction Codes is the best way to correct minor changes in features. There are two main types of (ECC) (Rashmi and Nag, 2013), Block codes like Hamming Codes, General Theory of Binary group codes, Low Density Parity Check (LDPC) Codes and Reed-Solomon (R-S)

Codes. Convolutional codes where the code words depend on the data message and a given number of previously encoded messages. For example Viterbi decoding, General Description of Convolutional Codes, Punctured Codes, Decoding and the Viterbi Algorithm and Turbo codes.

Reed-Solomon

The Reed-Solomon (R-S) codes are particularly useful for burst-error correction. Also, they can be used efficiently on channels where the set of input symbols is large. An interesting feature of the R-S code is that as many as two information symbols can be added to an R-S code of length n without reducing its minimum distance. This extended R-S code has length n + 2 and the same number of parity check symbols as the original code (Rashmi and Nag, 2013).

Combination between Biometrics and Cryptosystem:

This approach is using a combination between biometrics and cryptosystem. The importance of biometric technologies is shows in many fields such as security, authentication and monitoring applications.

This part presents the previous combination between biometric and cryptosystems. Many works are done on biometric cryptography in last few years most of the cases focus on single biometric and few of them focus on tow biometric.

P. Tiwari and A. Saklani in 2013 proposed a biometric based cryptography scheme, in which a master key is generated using whole/partial hash portion of combined sender and receiver finger print. Then generate as many random keys as they need from master key. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, Tai-hoon Kim in (2011) proposed system automatically acquires the biometric data in numerical format (Iris Images) by using a set of properly located sensors. Detect “IRIS Effective Region (IER)” and IRIS Edge by applying template in all numerical number in iris. Ajita Rattani', D. R. Kisku', Manuele Bicego and Massimo Tistarelli in (2006) Proposed system fuses the two traits at feature extraction level using two biometrics (face, fingerprint) in recognition. They used shift feature extraction. Sanjay Kanade, Dijana Petrovska-Delacr´etaz, and Bernadette Dorizzi in 2009 propose a two factor scheme to generate cancelable iris templates using iris-biometric and password. Using Hamming distance Error Correcting Codes (ECC) to correct the biometric data. Boult et. Al. proposed fingerprint based bio tokens which provide revocable templates. They employ robust matching techniques in encoded domain. They report an average decrease of 30% in the Equal Error Rate (EER) of the system. But, they do not provide any details about system performance when the transformation parameters are stolen. Feng Hao, Ross Anderson, John

Daugman in 2005 proposed integration between irises biometric with cryptographic applications. Using combination between Reed-Solomon and Hadamard code to cope with the 10 to 20% of error bits within an iris code and derive an error free code.

Proposed Work

This is the main part of this paper, the methodology and proposed work. This part is divided into three sections. The first section is talking about extracting features from three biometrics. The second one is talking about ECC and merging binary code together to retrieve 192 bit key. The final part is speaking about encryption/decryption techniques. These three parts is cleared in figure 6.

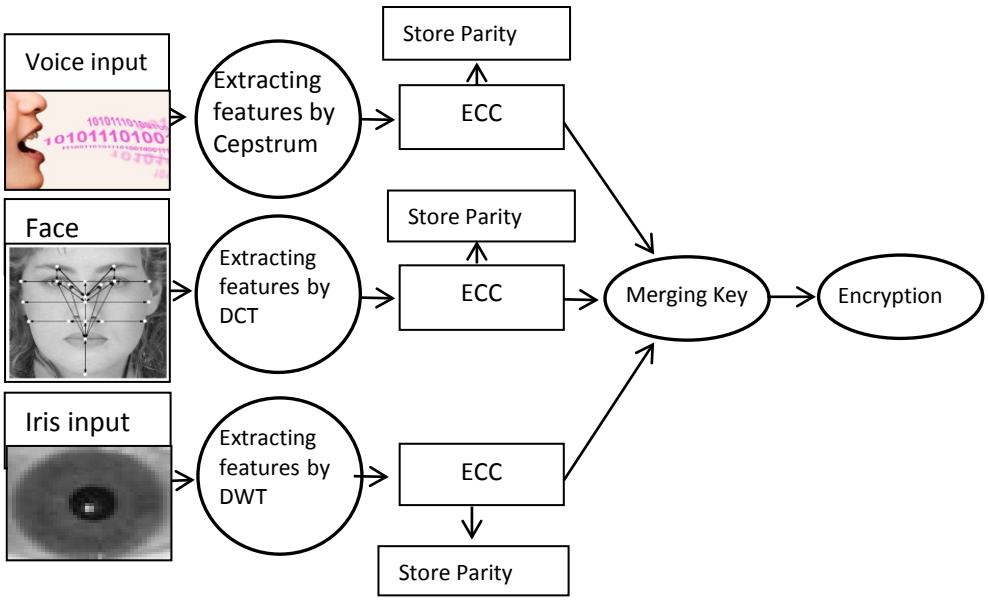

Figure 6: Encryption cycle

a. Features Extraction and Binarization

Extracting powerful feature is one of the most important parts to encrypt message and receiving correct data from encrypted message.

- **Voice Features Extraction**

Using voice samples with length not less than 1.5 seconds to extract sufficient feature with frame duration (30 ms) and frame shift (10 ms).

Using Pre-emphasis coefficient is to correct the filtering of the lips. Pre-emphasis refers to a system process designed to increase the magnitude of some frequencies with respect to the magnitude of other frequencies in

order to improve the overall signal-to-noise ratio. Using Pre-emphasis coefficient α = 0.97.

Applying cepstrum FT → abs () → log → IFT is to extract feature of the voice.

Choosing the mean value of the output features as threshold, this will convert decimal values into set of zeros and ones. Convert the output matrix into single column as shown in figure 7.

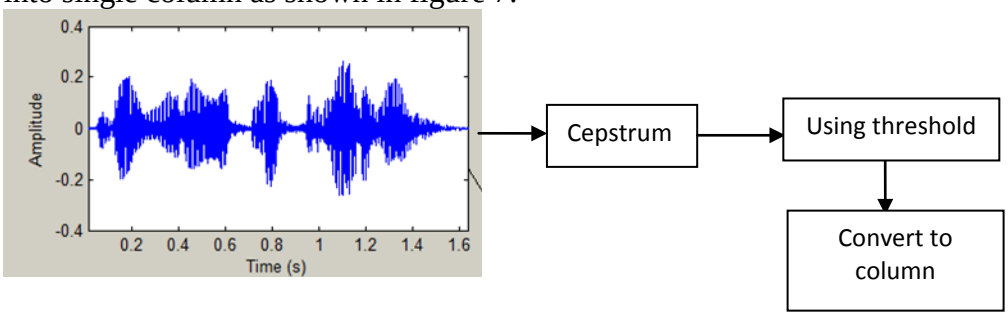

Figure 7: Voice features extraction.

- **Face Features Extraction**

Each image diminution is 180 * 200p equal 36000 features.

Resize the face image to be 10*10p and extract 100 features that is what the correction code required, to use all high and low features without using large amount of features.

Applying DCT2 on face images. The discrete cosine transform (DCT) is well-known_signal analysis tool used especially in compression standards due to its compact representation power (Aman, Pallavi and Mani 2011).

The definition of the DCT2 for an N * M input image A and output image B is:

$$\underset{\substack{0\le p\le M-1\\ 0\le q\le N-1}}{B_{pq}} = \alpha_p \alpha_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad (1)$$

Where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases} \quad (2)$$

And

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases} \quad (3)$$

Removing the top-left part of the basic functions Eq. 1, the (0, 0) component that contain the average intensity value of the image, which can be directly affected by illumination variations figure 8.

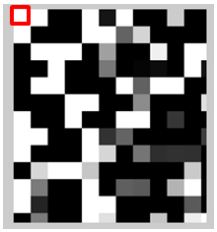

Figure 8: The (0, 0) component - the average intensity value

Extracting features from face using discrete cosine transform does not require detection of any local regions, such as eyes, nose and mouth, as in the modular or component based approaches (Hazım and Rainer 2006; Bernd, Purdy, Jane and Tomaso, 2003) for face representation.
After using DCT2 the low feature of the image is store in upper left corner and high feature that contain edges and high details in the rest of the image shown in figure 9.

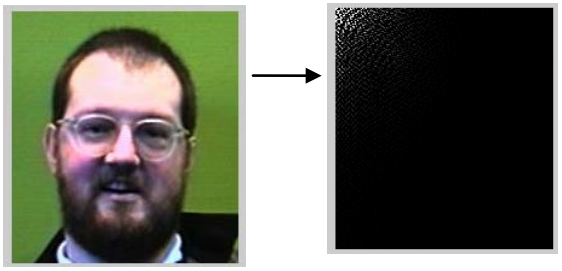

Figure 9: DCT Image transformation.

Convert the output matrix into single column. Features extraction is shown in figure 10.

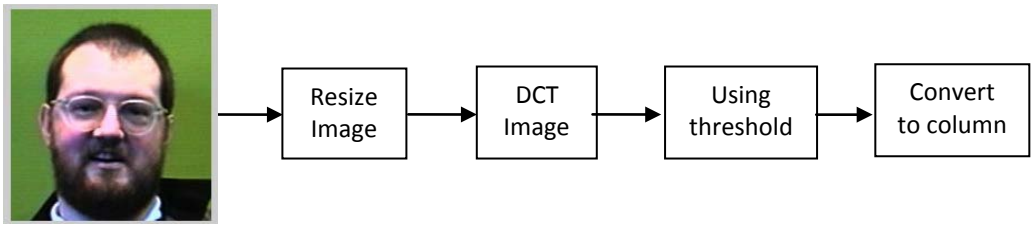

Figure 10: Face feature extraction.

- **Iris Features Extraction**

The iris image dimensions are 768*576p. Applying circle mask with radius 320p to remove the outer part of the eye and eye lashes.

Resize the image to use all feature of the iris and to be 10* 11p to extract 110 features from iris image.

DWT2 Coiflets family was applied to extract features from iris then convert the output two dimensions matrix into single column as shown in figure 11.

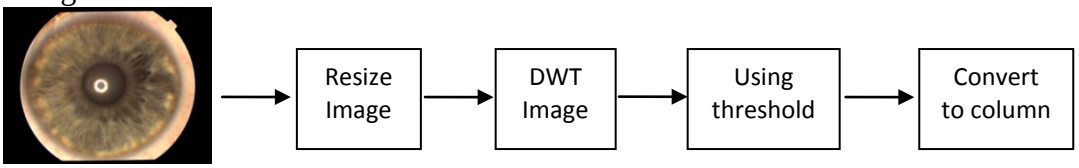

Figure 11: Iris features extraction.

b. Error Correction Code and Merging Extracted Features

Using Reed-Solomon to extract parities from each biometric and store it to reuse it in decryption cycle.

Combining extracted binary feature from biometric by using AES encryption technique and using the multiple mixing, substitutions and permutation.

Shifting given key in ASE to generate new key then using extracted key as data in ASE.

c. Encryption/Decryption

Using Triple DES is to perform an encryption.

Dividing the key extracted from merging section into three parts each part containing 64 bit for each round of triple DES shown in figure 12.

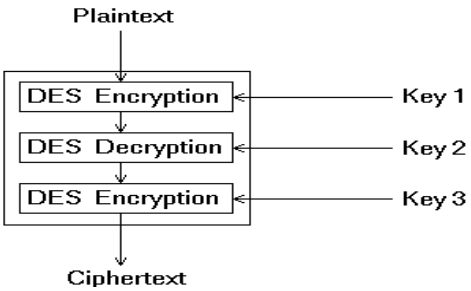

Figure 12: Triple DES.

Storing the encrypted message (cypher text) was to use it in decryption cycle to retrieve the original message (plain text). Decryption cycle showed in figure 13 using the same steps in encryption cycle except not store the parities but using it to retrieve the correct key.

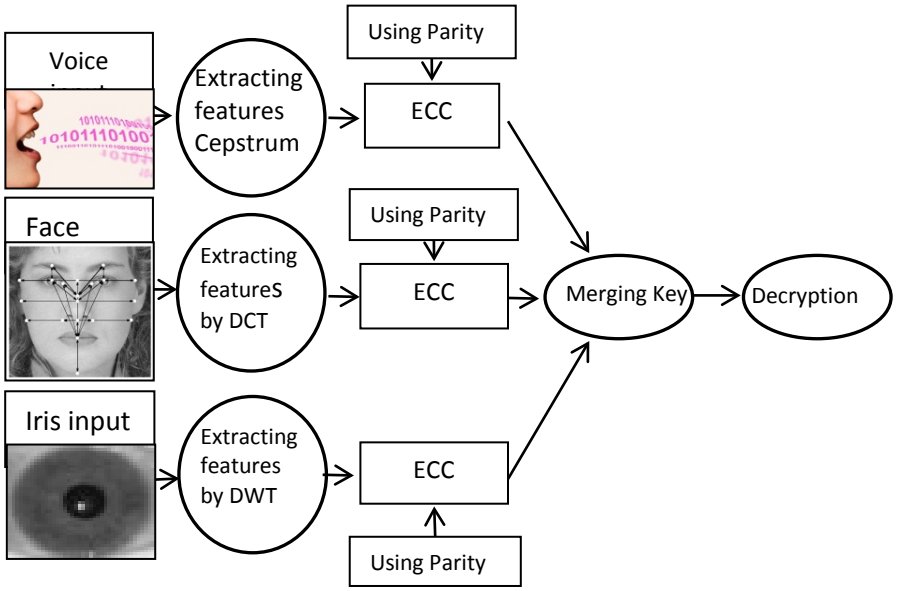

Figure 13: Decryption cycle

Experimental Results

The data base was built from three sets voice, Iris and Face. Each set contains three samples from 20 persons. Voice DB was collected manually from 20 person each person has three voice samples. These samples were collected from men and women with different ages. The face DB contain 30 person each person has 20 images. The 20 persons and the 3 images for each person were chosen randomly from different genders and ages. The iris DB contains 100 persons each person has 3 iris images. The 20 persons were chosen randomly. First sample from each person is the reference sample. The second tow samples are the test samples. For each sample total number of elements was 127 elements.

- **Face Results**

Correct samples using Reed-Solomon, then compare each sample with other samples to find best number of correction elements. Table 1 and figure 14 show that after correct 18 elements reach the desired result. The accuracy after correction is 90.2%.

Table 1: Face ROC curve

Cut point	0	3	5	8	11	13	18	23	28
FPR	0	0.001	0.022	0.03	0.05	0.08	0.13	0.23	0.84
Sensitivity	0	0.37	0.62	0.70	0.87	0.98	1	1	1

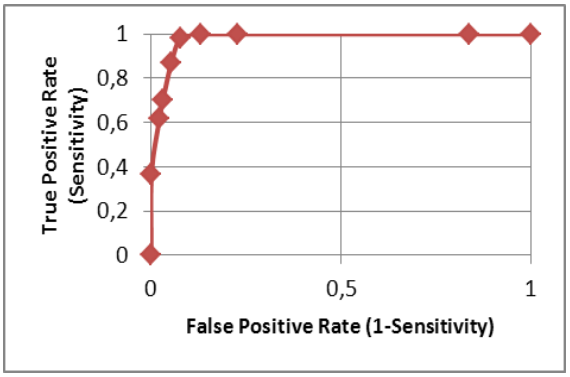

Figure 14: Face ROC curve

- **Voice Results**

After correct samples by Reed-Solomon, each sample was compared with other samples to find best number of correction elements. Table 2 and figure 15 show that after correct 23 elements reach the desired result. The accuracy after correction is 73.8%.

Table 2: Voice ROC curve

Cut point	0	5	10	15	18	20	23	28	33
FPR	0	0.001	0.012	0.07	0.27	0.42	0.59	0.90	0.93
Sensitivity	0	0.37	0.47	0.60	0.88	0.98	1	1	1

Figure 15: Voice ROC curve

- **Iris Results**

Correct extracted features using Reed-Solomon, and then compare each sample with other samples to find best number to correct elements. Table 3 and figure 16 show that after correct 17 elements reach the desired result. The accuracy after correction is 82.6%.

Table 3: Iris ROC curve

Cut point	0	3	8	11	14	17	20	23	26	29
FPR	0	0.05	0.19	0.34	0.51	0.65	0.74	0.84	0.98	1
Sensitivity	0	0.47	0.82	0.93	0.98	1	1	1	1	1

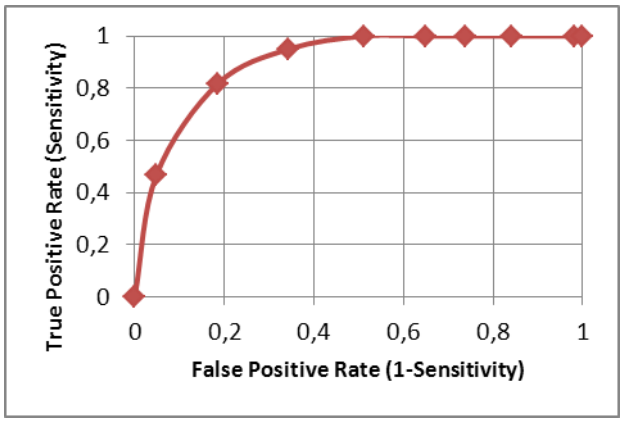

Figure 16: Iris ROC curve

By combining two biometrics the accuracy increased to be 92.45%. After using iris, voice, and face together the accuracy percentage grew up to be 99.83 %.

Time consumption for ECC

Table 4 and figure 17 show that the time consumption in Reed-Solomon ECC for different G.F 2^m is increased rapidly when then number of G.F increased by one.

Table 4: Time consumption for ECC

G.F correction	2^7	2^8	2^9
Time	1.775	16.431	557.459

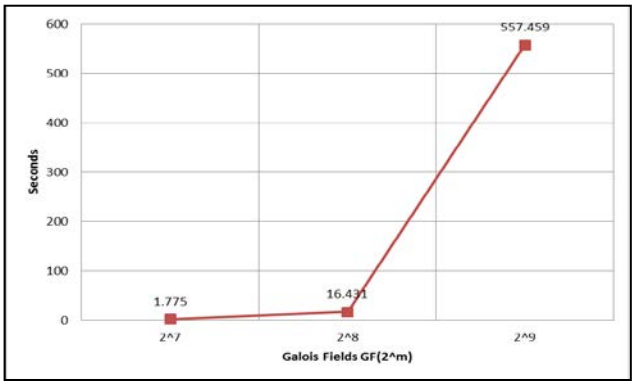

Figure 17: Time consumption for ECC

In this approach no need to use more than G.F 2^7 in ECC. Reed-Solomon with G.F 2^7 can correct up to 31 elements after exclude the 64 elements from each biometric with percentage 48%. The required percentages to reach the correct sample are 28%, 35% and 17% for face, voice and iris respectively. The time consumed by combining the 3 biometrics is 6 seconds. Using one biometric with 192 features will increase accuracy percentage, but it needs large number of correction. The maximum percentage by using RS with G.F 2^8 is 32% it cannot correct voice samples. In this case must choose RS with G.F 2^9. The time consumption by using one biometric and extract 192 features then correct features is 560 seconds. In case that RS with G.F 2^8 is sufficient to correct samples, the time consumed are 18 seconds 3 times more than using combination approach.
Figure 18 shows the final output for the proposed work "Biometric Cryptosystem".

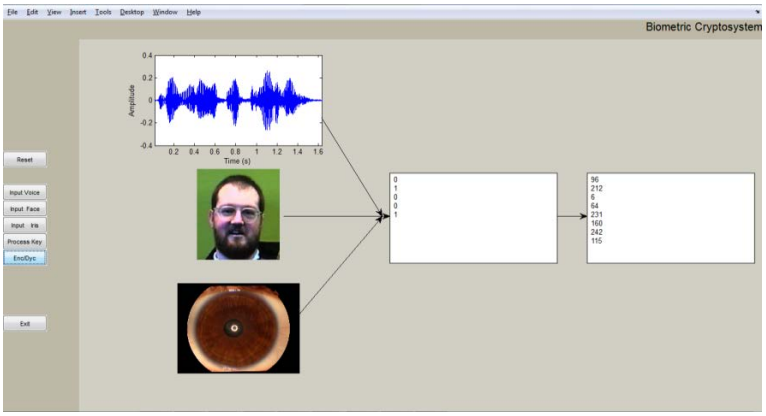

Figure 18: Biometric Cryptosystem

Conclusion

"Cryptosystem from Multiple Biometric Modalities" proposed a novel approach using multiple biometric in cryptosystem for produce a very strong way in cryptography. This approach is using error correction code (ECC) as way to reducing variability that was generated from extracted codes from voice, face and iris (that is treated as errors). In this study the ECC was designed by using Reed-Solomon code carefully to overcome errors that generated from biometrics. Moreover, the corrected codes from biometrics were merged together. This merging separates the input biometric from key that used in cryptography and increases the hamming distance for intruder. The output key can only be generated by using parity code that is stored with user which makes the system truly revocable. In this approach there is no any template or any personal biometric data stored so the impostor cannot find any data to steal. This system was tested by large amount of data to extract correct number of correction parity for each biometric.

After fine-tuning and get the correct parity, the data was divided into groups each group contains 3 samples from same person and tested with other persons. When using only face the percentage is 90.2%. When using voice the percentage is 73.8%. When using Iris the percentage is 80.6%. After combining two biometrics the accuracy increased to be 92.45%. After using iris, voice, and face together the accuracy percentage grew up to 99.83 %. The proposed system improves the performance from other biometrics by reducing errors from biometrics to be less than 0.17 %.

References:

Srivastava, P.C., Agrawal, A., Mishra, K.N., Ojha, P. K. and Garg, R. (January 2013) "Fingerprints, Iris and DNA Features based Multimodal Systems: A Review" I.J. Information Technology and Computer Science, Volume 02, pp.88-111.

Tico, M. (November 2001) "On Design and Implementation of Fingerprint-Based Biometric System" Ph.D. dissertation, Tampere Univ. of Technology, Finland.

Gaikwad, S.K., Gawali, B.W. and Yannawar, P. (November 2010) "A Review on Speech Recognition Technique" International Journal of Computer Applications Volume 10.

Hao, F., Anderson, R. and Daugman, J. (September 2006) "Combining Crypto with Biometrics Effectively" IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088.

Shaojun Zhu (September 2009) "Facial Feature Points Extraction" Image and Graphics, 2009. ICIG '09. Fifth International Conference, pp. 195 – 199.

Seung-In Noh, Kwanghyuk Bae, Yeunggyu Park, and Jaihie Kim (June 2003) "A Novel Method to Extract Features for Iris Recognition System", 4th International Conference, AVBPA 2003 Guildford, UK, pp. 862–868.

Anderson, R., Wiley, J. and Sons (2010) "Security Engineering: A Guide to Building Dependable Distributed Systems" Chapter5, pp. 73 – 95, 2nd Edition.

Dhotre, I.A. and Baga, V.S. (2008) "Data Communication and Networking: A Practical Approach" Chapter 5, pp.137 – 143.

Rashmi and Nag, V.R (2013) "Performance study on the suitability of Reed Solomon codes in communication systems" CT International Journal of Information &Communication Technology Vol. 1, Issue 1.

Tiwari, P. and Saklani, A. (May 2013) "Role of Biometric Cryptography in Cloud Computing" International Journal of Computer Applications Volume 70– No.9.

Sushmaja, K. and Dr. Fazal Noorbasha (April 2013) "Fault Detection with Error Correction Codes for Memory Applications" International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 2, pp.392-395,.

Bhattacharyya, D., Das, P., Bandyopadhyay, S.K. and Kim T. (2011) "IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition" International Journal of Database Theory and Application pp.53 – 60.

Ajita Rattani, Kisku, D. R., Manuele Bicego and Massimo Tistarelli (August 2006) "Robust Feature-Level Multibiometric Classification" Biometric Consortium Conference, Biometrics Symposium: Special Session on Research, pp.1 – 6.

Sanjay Kanade, Dijana Petrovska-Delacr´etaz and Bernadette Dorizzi (June 2009) "Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce variability in biometric data" IEEE Conference on Computer Vision and Pattern Recognition, pp.120-127.

Boult, T.E., Scheirer, W.J. and Woodworth. R. (June 2007) "Revocable Fingerprint Biotokens: Accuracy and Security Analysis" IEEE Conference on Computer Vision and Pattern Recognition, pp.1 – 8.

Aman R. Chadha, Pallavi P. Vaidya and M. Mani Roja (2011) " Face Recognition Using Discrete Cosine Transform for Global and Local Features" International Conference on Recent Advancements in Electrical, Electronics and Control Engineering, Vol. 43 no. 3 pp.167-188.

Hazım Kemal Ekenel and Rainer Stiefelhagen (July 2006) "Block Selection in the Local Appearance-based Face Recognition Scheme" IEEE Conference on Computer Vision and Pattern Recognition Workshop, pp.43 – 50,

Bernd Heisele, Purdy Ho, Jane Wu and Tomaso Poggio (July 2003) "Face recognition: component-based versus global approaches" Computer Vision and Image Understanding pp.6 – 21.