Key Generation Based on Facial Biometrics

Ielaf O. Abdul Majjed [1], Alyaa M. Abdul Majeed [2]
{ Ie_osamah@uomosul.edu.iq [1,] alyaahaleem@uomosul.edu.iq [2] }

College of computer sciences and mathematics, University of Mosul[1,2]

Abstract. Over the past few years, advances in communication technology have brought large amounts of digital data to ordinary media, which required the development of computer security technologies. In this work, we suggested a new method to generate a biometric key to encrypt data using the properties of the human face, then used this key to encrypting speech messages and hide them inside the colored images. This can be achieved depending on splitting the facial image into two parts (upper and lower parts) and then generated a unique encryption key using Maximum-Relevance Minimum Redundancy (mRMR) feature selection algorithm from the upper part after that encrypted the original speech message using two levels, in the first level we used Arnold cat map to permutation the samples then in the second level used bio-key to encrypting the message and then hide the encrypted speech message in the lower part of the facial image. In order to determine the efficiency of the proposed method, different measures were applied (correlation coefficient, PSNR, MSR, SSIM).

Keywords: mRMR, speech, Arnold cat map, boi-key, facial image.

1 Introduction

In recent years, tremendous increase and unexpected interest and development in securing communication technologies has occurred. To achieve secure transmission and ensure that data is delivered to the targeted authorities, the process must be accessible through a common network. Therefore the need was arisen to develop encryption technologies to achieve a high level of security by making the data unclear to people who are not authorized to receive the data, Consequently, the attacker who captures the encrypted data passed through the shared network will not able to read it and still unable to create meaning or change the data in an undetectable manner [1][2]. Existing asymmetric encryption algorithms require a secret key. Passwords used to protect the keys are often weak and can be easily attacked and obtained by brute force. Combining biometrics and coding is, however, possible solution. Though, in order to obtain consistent keys, any bio coding system should have the ability to eliminate the small differences that exist between different acquisitions of the same biometrics. In general, using an encryption system causes different issues, and has some related disadvantages, such as [1], Conventional encryption relies on key-based message authentication, without user dependency. Therefore, it cannot differentiate between the original user and the attackers. The keys used can be guessed or broke by the attacker.

- The encryption / decryption process requires a longer delay due to the large size of keys.
- The keys are saved in an unsafe database because they are difficult to be remembered.
- Additionally, maintaining and sharing arbitrary keys is a critical issue in cryptographic frameworks.

IMDC-SDSP 2020, June 28-30, Cyberspace

DOI 10.4108/eai.28-6-2020.2298074

Biometric is a measurable and statistical test of a person's physical and behavioral attributes. The most common physiological features used for biometrics are faces, fingerprints, and ears[3]. The behavioral features that can be measured can include rhythm, rule, gestures, and speech [3]. Using very unique properties for describing good biometrics is important to ensure that the quality of the feature does not change over time and the users are comfortable and avoid distorting this feature. A cryptographic biometric system can work in one of three accompanying ways: key release, key binding, or key generation[4].

When the keys are released, the biometric code and the key are stored as a separate entity. In the key binding mode, keys and modes remain integrally within the cryptographic scope. It is computationally infeasible to decrypt a key or template without knowing the user's biometrics. A cryptographic biometric matching method can be used to complete the verification and release the key in one step[3][4]. In this paper, we use a key generation method where the key is directly extracted. from the biometric data and not stored in the database.

2 Related Works

A.O. Abdul-Majeed in [5] applied Arnold cat's map transform on an image in several encryption levels thus, the image is broken into several crossed blocks started from center and incrementally grow in the size. Arnold cat's map was applied in every level along with zigzag scan which was implemented over the entire image to lessen the pixel correlation. To fulfill the diffusion concept, random generated values are xored with image pixels in every level. The secret keys were the control parameters and the iteration number of the Arnold cat map as well as the initial seed. In another scope, Yang et al [6] used five real datasets to implement the mRMR feature selection method that selects maximal statistical feature depending on mutual information (MI). The author discussed redundant features and relevant features simultaneously. On the other hand, new speech encryption system was introduced by Alyaa [7] That system was based on genetic algorithms (GA) and Arnold cat map, and included maps in order to increase the security. The encrypted speech signal was difficult to be easily recovered from an intruder because it had a more scrambled form. The recovered speech quality was good with low residual intelligibility for an encrypted message.

3 Proposed method

In this proposed method, to utilize one of the facial biometrics that distinguishes individuals from others, facial images were used to hide encrypted voice messages using biometric keys extracted from the same facial image. In order to implement this proposed method, many steps were performed (**Figure 1**).

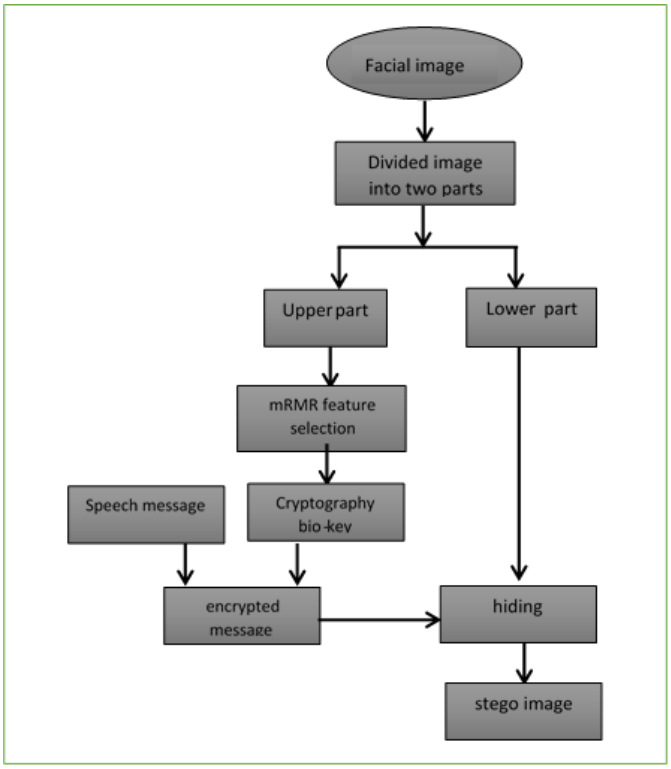

Fig.1 proposed method block diagram

3.1 Cryptography bio-key generation

The facial image was separated into two parts (upper and lower) a unique encryption bio-key was created using mRMR method from the upper part

3.1.1 mRMR feature selection

Peng et al. proposed mRMR feature selection method [6]. The mRMR is a process that tends to select features with low correlation between features, but high correlation with categories. In order to maximize the objective function, a greedy search was used to select features one by one [7] [8].

3.2 Speech message encryptions.

This article used two levels to encrypt the voice signal (**Figure.2**):

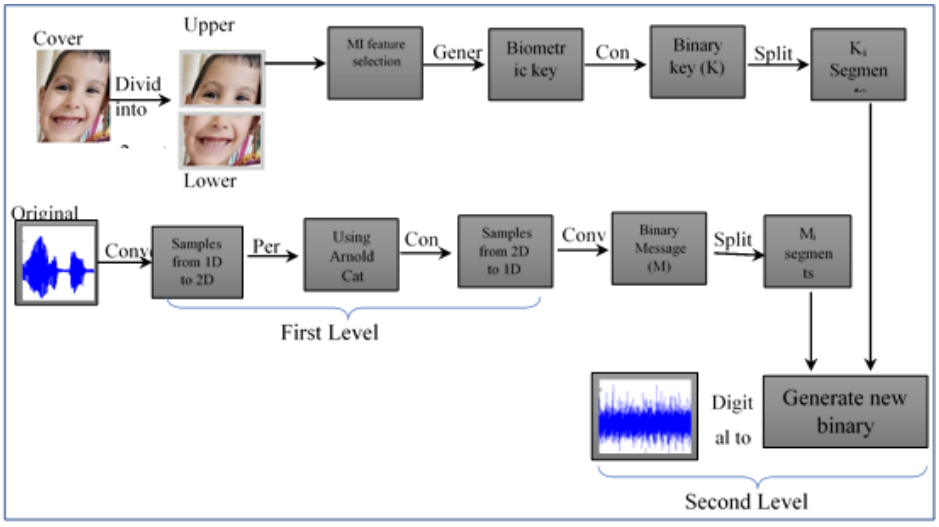

Fig.2 speech message encryptions block diagram

3.2.1 First level

At this level, the process of scrambling speech signal samples is performed in the time domain, where the samples were converted from a one-dimensional vector to a two-dimensional matrix. A scrambling key was then generated to replace the position of the speech signal samples. The process was performed using Arnold's cat diagram using the following mathematical formula:

$$\begin{bmatrix} R_{M+1} \\ C_{M+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \cdot \begin{bmatrix} R_M \\ C_M \end{bmatrix} mod(M) \qquad (1)$$

Here, a and b were control parameters of positive integers, R_M, C_M were the positions of the original samples in the M × M matrix, R_{M+1}, and C_{M+1} were the new location after applying the Arnold cat map, and to encode the message, Arnold cat map can be executed N times, which caused reappearing of the sample in its original location (there were T positive integers such that $(R_{M+1},C_{M+1}) = (R_M,C_M)$) where N depends on the parameters a, b and the size of the sample matrix (M × M). [9]

The scrambling process completed multiplying the position of each sample by transforming Arnold's cat. Repeating the new positions of the sample generated after iterating the Arnold cat figure (**Figure 3**).

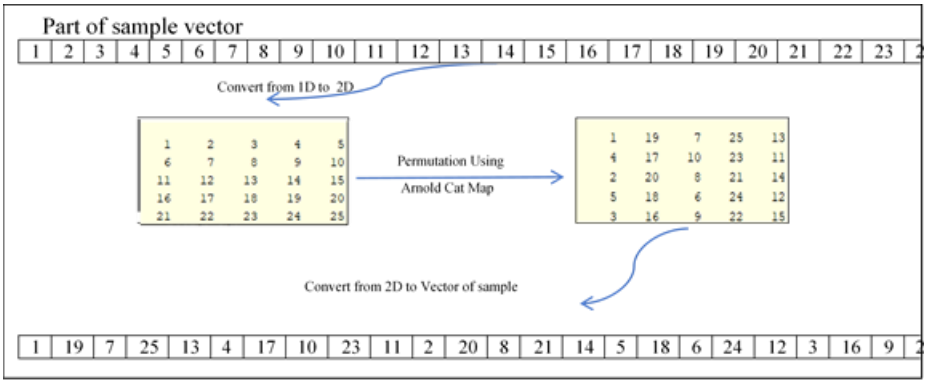

Fig.3. permuted sample using Arnold Cat Map block diagram

3.2.2 second level

The process used for permute speech samples bits using the bio-key that generate in step1 is described as the following (**Figure** 3.):

1. Convert of bio-key into a binary sequence (K).
2. Divide the K into a segment of the same size and generate Ki segments.
3. Convert of each sample of the encrypted message into binary and generate M- bits message.
4. Divide the M message into segment Mi.
5. Insert of each Mi of M before Ki to produce a new binary sequence (MiKi).
6. Divide the MiKi into a segment with a size equal to the size of original samples, then convert of binary sequence to decimal.

4 Hidden the encrypted speech message

In the proposed method, an encryption signal was hidden using the following step (**Figure 4**):

Step1: LP (lower part) is a cover image (RGB), was altered to embed encryption message.

Step2: the Mask byte (M) was shared between the sender and the receiver.

Step3: LP cover image (Red Palate) was partitioned into the blocks of size 8 x 8.

Step4: encrypted message was divided into a frame of size 64 sample then convert each frame form 1-D to 2-D of size 8*8.

Step5: the sample value of each block was converted into binary.

Step6: the pixel of each block was converted into binary.

Step7: bitwise AND operation was performed on each pixel of block with mask.

Step8: Perform bitwise AND operation of each sample of block with mask.

Step9: Perform LSB substitution process between sample and pixel for each pixel and sample in the block.

Step10: steps 5 to 9 were repeated until the end of all block of encryption message.

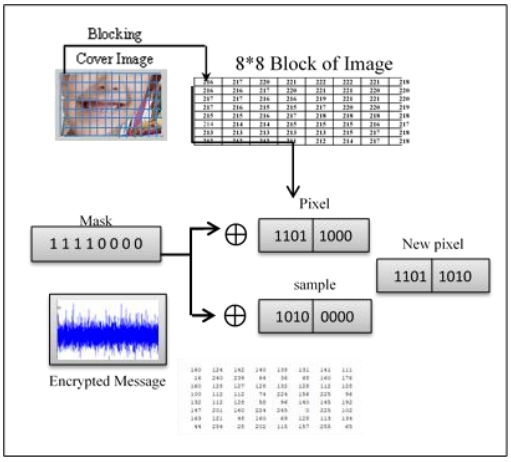

Fig 4: encrypt speech message hiding block diagram

5 Results of the experiments

In this part, we proceed with an experimental analysis of the proposed method. Figure 5 shows the 512×512 RGB image and its histogram used to hide speech signal before and after embedding. Several objective tests are used to measure the quality of an image after hiding an encrypted speech message such as correlation coefficient, PSNR,
MSR, and SSIM. The method has been thoroughly tested on 5 images and hidden an encrypted message with three different file size, sample size and sampling rates (tables 1,2, and 3)

As shown in the tables, the method has a maximum PSNR equal to (64.8178) when the number of samples that were hidden was 40000, and it equal (62.8072) when the number of samples that were hidden was 23104, but it will be (62.7364) when the number of samples is 19881 at implementing them on the same image.

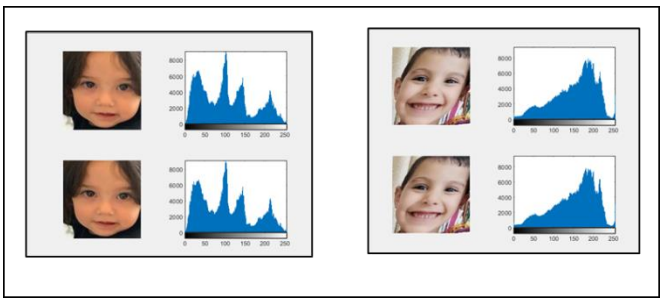

Fig 5: histogram for coved and stego image

Table1: The size of encrypted message (sound1) that hidden in 512*512 image is 40000 samples (230000bits)

image_name	MSR	PSNR	SSIM	Correlation coefficients
Aws1	0.0567	63.2569	0.9993	0.99998
Aws2	0.0435	63.5444	0.9996	0.99995
Pamo1	0.0418	63.7897	0.9984	0.9998
Pamo2	0.0481	64.8178	0.9994	0.99996
Stand	0.0496	64.4924	0.9971	0.9997

Table2: The size of encrypted message (sound2) that hidden in 512*512 image is 23104 samples (184832 bits)

image_name	MSR	PSNR	SSIM	Correlation coefficients
Aws1	0.04833	60.833	0.9989	0.99997
Aws2	0.0753	61.4725	0.9994	0.99992
Pamo1	0.0795	61.5212	0.9973	0.9997
Pamo2	0.0772	62.8072	0.9987	0.99994
Stand	0.0651	62.7704	0.9995	0.9998

Table3: The size of encrypted message (sound3) that hidden in 512*512 image is 19881 samples (159048 bit)

image_name	MSR	PSNR	SSIM	Correlation coefficients
Aws1	0.0790	60.6737	0.9989	0.99992
Aws2	0.07239	61.5117	0.9994	0.99992
Pamo1	0.08020	61.5357	0.9973	0.99978
Pamo2	0.07447	62.7364	0.9987	0.99994
Stand	0.0647	62.5391	0.9996	0.9998

Figure 6 displays the waveform layout of the original, encrypted (level 1 and level 2) and the recovered signal after retrieving it from the stego image and decrypted respectively which resulted from the application of the proposed system. Table 4 illustrates the results for the quality of three recover signals.

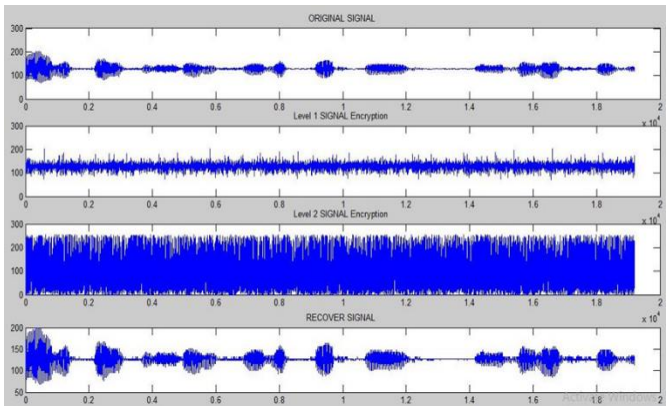

Fig 6: original speech message, encrypted speech message (level 1 and level 2) and recover speech signal

Table 4: Performance measures of quality for recovered signal

Signal	NRMSR	PSNR
Man	1.1237	66.9042
DISH38	1.1464	57.3338
Hh	1.1348	54.3199

5 Conclusions

The encryption key created in this work with the biometric is complex and stable throughout a person's life so is a very limited risk of losing, theft or falsification of the user's biological identity. The Experimental results indicated that the proposed method for encrypting the original speech signal at two different levels, then hide it in the cover image has the following characteristics: good confusion and proliferation properties, large enough area for the encrypted key length, a high level of security, and uniform distribution of hidden samples within the image. After analyzing the results, it is clear that the proposed algorithm has high security that was achieved using two levels of encryption and steganography level to make it difficult to be broken by the attacker. This system provides better PSNR, MSE, SSIM and correlation which improves steg-image quality.

References

[1] Rashi Bais, K.K.Mehta ,"Biometric Parameter Based Cryptographic Key Generation " ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June (2012).

[2] Brent Carrara and Carlisle Adams, "You are the Key: Generating Cryptographic Keys from Voice Biometrics", (2010) Eighth Annual International Conference on Privacy, Security and Trus.

[3] Mr.P.Balakumar and Dr.R.Venkatesan , "A Survey on Biometrics based Cryptographic Key Generation Schemes", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No. 1,(2012).

[4] Dr.R.Seshadri,T.Raghu Trivedi, " Efficient Cryptographic Key Generation using Biometrics" , Int. J. Comp. Tech. Appl., Vol 2 (1), 183-187.

[5] Abdul-Majeed, Ansam, "Chaotic Scheme for Image Encryption Based on Arnold Cat's Map", International Journal of Computer Science and Information Security, 12. 26-33, (2014).

[6] Yang J, Zhu Z, He S, Ji Z. "Minimal-redundancy-maximal-relevance feature selection using different relevance measures for omics data classification", IEEE symposium on computational intelligence in

bioinformatics and computational biology (CIBCB). New York: IEEE; p. 246–51, (2013).

[7] Haleem, Alyaa, "Speech Encryption Using Genetic Algorithm and Arnold cat map", International Journal of Computer Science and Information Security ,Vol. 14, No. 12, 911-915,(2016).

[8] H. Peng, F. Long, and C. Ding, "Feature selection based on mutual information: criteria of max-dependency, max-relevance, and minredundancy," IEEE Transactions on Pattern Analysis & Machine Intelligence, no. 8, pp. 1226–1238,(2005).

[9] Milos Radovic1, et al, "Minimum redundancy maximum relevance feature selection approach for temporal gene expression data", Radovic et al. BMC Bioinformatics, DOI 10.1186/s12859-016-1423-9,2017.

[10] Jo, & Lee, Kunwoo & Oh,. (2019). "Improved Measures of Redundancy and Relevance for mRMR Feature Selection". Computers. 8. 42.,2019.

[11] Eko Hariyanto , Robbi Rahim ,"Arnold's Cat Map Algorithm in Digital Image Encryption", Article in International Journal of Science and Research (IJSR) • October 2016 DOI: 10.21275/ART20162488.