Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 1, January 2021, pp. 208~214
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i1.pp208-214

Biometric key generation using crow algorithm

Zied O. Ahmed, Abbas Akram Khorsheed
Computer Science Department, Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received May 7, 2020
Revised Jul 6, 2020
Accepted Jul 27, 2020

Keywords:

Biometric
Crow search algorithm

ABSTRACT

The researchers have been exploring methods to use biometric characteristics of the user as a replacement for using unforgettable pass-word, in an attempt to build robust cryptographic keys, because, human users detect difficulties to call up long cryptographic keys. Biometric recognition provides an authentic solution to the authentication of the user problem in the identity administration systems. With the extensive utilization of biometric methods in different applications, there is growing concern about the confidentiality and security of the biometric technologies. This paper proposes biometric based key recreation scheme. Since human ears are not correlated. Until now, the encryption keys are generated using a swarm intelligence approach. Collective intelligence of simple groups of autonomous agents have been emerged by swarm intelligence. The crow search algorithm which is known as (CSA) is a new meta-intuitive method assembled by the intelligent group behavior of crows. Despite that CSA demonstrates important features, its search approach poses excessive challenges while faced with great multimodal formularization.

Corresponding Author:

Zied O. Ahmed
Computer Science Department
Mustansiriyah University, Baghdad, Iraq
Email: zied_othman@uomustansiriyah.edu.iq

1. INTRODUCTION

Biometrics can be defined as the science of creating an individual's identification based on a person's physical, chemical or behavioral features [1]. Due to the properties of the biometric particular nature [2] and the undeniable it offers [3], biometry can be often used to improve the general security of the system to which it is applied: authentication system encryption system of biometric. The authentication of biometric can be explained as the procedure of verifying the singularity of human in accordance with his/her physiological features or behavioral characteristics [4]. Fingerprint, an iris or a face are the Physiological characteristics, which refers to something that represent an individual. Whereas speech, keystroke and signature dynamics are the communicative behavioral characteristics which refers to something that can be done by individual. As stated by Biggio [5], the common integrated biometric authentication system works as the following procedure. An individual provides his/her identity to access to any resource. The sample of the user's biometric has been taken by the sensor. Properties are obtained by the sample and a resemblance percentage can be calculated between the two samples, first sample is the biometric which has been provided and the second is the sample that has been stored in the biometric pattern data-base correspondent to the identity of the user which has been provided. The resemblance percentage is contrasted to the threshold in order to identify the user is as real or a fake. According to this determination, the access is granted or rejected to the resources. Biometric encryption systems including the key generation and the key binding systems, incorporate the highest level of security provided by rejection supplied by biometry and cryptography. The systems of key generation can be known as those systems that create a stable encryption key obtained by

biometric data [6, 7]. The systems of key binding systems can be known as the systems that can bind an encryption key, which has been generated randomly to the biometric pattern [8, 9]; the bound key is left to apply upon a logical presentation of the proper biometric model. The biometric samples that have been stored create a risk to the users' privacy.

The crow search algorithm (CSA) can be defined as a meta-heuristic way where users imitate the behavior of being intelligent in a pack of crows. The results which have been published show the capability to find a solution for a different complicated engineering optimization difficulties. Some cases comprise image processing in addition to its application to water resources. Although it has important results, its search scheme poses considerable challenges when faced with the highest multi-modal formulations [10]. Chang et al. [11] have declared their proposal about a framework for generating a stable cryptographic key based on single mode biometric properties which are volatile in nature. The main article of their research is the procedure to producing properties of distinguishable biometric, which results in a strong cryptographic key. Although the framework performance which has been proposed can be estimated with a face data-base that including the expressions of the face and the head movement differences, the authors have announced that it applies to other biometric methods as well as the framework.

According to the Reed-Solomon algorithm, Wu et al. [12] have improved a new system for face biometric encryption by using 128 dimensional primary component investigation vector and error correction codes which has known as (ECC). In the decryption step, a biometric key is resulted by using the look-up table generated during the step of encryption, while the final key can be achieved by utilizing the biometric key with the ECC. Feng Hao et al. [13] have submitted a cryptographic key method based on biometric by using the iris characteristic. According to the authorized codes of iris, a periodic string of binary entitled as a biometric key has been generated in order to be more authentic. Extra data of error correction that does not unvei006C the key and can be accumulated in a type of tamper-resistant because a smart card is utilized to generate the key according to an individual's iris image. Beng.A et al. [14] have proposed a randomized biometric assistant according to a biometric key generation pattern. This technique comprises a password backup structure and a random feature discretization procedure. First, it allowed errors to be minimized, any other way, the later tested intra-class differences of biometric data compared with the minimum. The unsystematic biometric assistant demonstrated which it is easy to override a biometric key as soon as the key becomes clear.

Mishra and Bali [15], have presented an application of genetic Algorithm in the cryptography field. Key selection is a selection procedure in which keys has been classified according to their suitability which has happened within the public key encryption. Ultimately, it generated the most random and unrepeatable final keys, which have raised the robustness and security of the keys. Jhajharia et al. [16] have proposed an algorithm of public key cryptography (PKC) based on the composite principle of the two developed algorithms, which are particle swarm optimization (PSO) and genetic algorithm (GA) consecutively. These algorithms can be used to generate the more relevant fine fit keys in the field including the finest keys with the highest strength. Abu-Mouti and Elhawary [17] has declared an overview of the utilize of the literature of an Artificial which is known as bee colony (ABC) algorithm, which is a meta-heuristic based on a population improvement procedure obtained by the intelligent feeding behavior of honey bee flocks. The performance features and basic properties of the ABC algorithm are also explained.

Sanaul Hoque et al. [18] have presented the direct generation of the biometric keys from live biometrics, under certain conditions, by partitioning feature space into subspaces and partitioning these into cells, where each cell subspace contributes to the overall key generated. They assessed the presented technique on real biometric data, instead of both genuine samples and attempted imitations. Experimental results have proved the reliability in possible practical scenarios for this technique. A et al. [19]. The technique engrosses a randomized feature discretization process and a code redundancy construction. The former method controls the intra-class variations of biometric data to the nominal level and the latter reduced the errors even more. The randomized biometric feature was proved as a simple technique, when the key was conciliated The projected technique was assessed in the context of face data based on a subset of the facial recognition technology (FERET) database.

2. THE CROW SEARCH ALGORITHM (CSA)

The pensive observation of some living beings' behavior can demonstrate how they plan their ordinary behavior to algorithmic standards. These algorithms are comprehensive optimization meta-heuristics which can be basically composed by selecting the most usefully scheme and a random structure. Previous guidelines eliminate both loss of diversity and algorithm to limit both local loss and the algorithm that combines optimal use. Global optimality success can be obtained by a good stability of the use and investigation [20]. The crow search algorithm (CSA) is a recent metaheuristic method based on the intelligent

group behavior of crows. Although CSA presents interesting characteristics, its search strategy presents great difficulties when it faces high multi-modal formulations [21]. The recent metaheuristic algorithm which is crow search algorithm has been developed by Alireza Askarzadeh [22], it is inspired by the crow intelligent behavior. Normally, crows prove the intelligence behaviors as self-realization, discriminating faces, stimulating the influx of possibly hostile ones, advanced ways of communication, and reminding the secret place of food after a period of time. All these behaviors can be connected to the truth that the crows' brain-to-body ratio is less than that of the human brain which can be considered one of nature's smartest birds a little bit [23].

The CSA evolutionary procedure imitates the crows' behavior of hiding and regaining more food. As an algorithm that based on population, the flock's size is confirmed by N individual (crow) whose problem size is n-dimensional n. The position k of Crow i in any given iteration k is described in (1) and represent a possibly problem solution [23].

$$X_{i,k} = \left[x_{i,k}^1, x_{i,k}^2, \dots, x_{i,k}^n\right] i = 1,2,3\dots,N;\ k = 1,2,\dots max\ Iter \quad (1)$$

where maxIter is the utmost iteration within the procedure. Each crow individually is supposed to be able to remember the most suitable visited the location of Mi,k to conceal food until the present iteration which described in (2) [23].

$$M_{i,k} = \left[m_{i,k}^1, m_{i,k}^2, \dots, m_{i,k}^n\right] \quad (2)$$

The location of each iteration is moderated based on Pursuit and Evasion behaviors[24]. Pursuit: A crow j comes after Crow i to find its secret place. While crow i does not watch out the existence of the following crow, as a result of crow j to obtain the purpose [24]. Evasion: The crow i notices crow j existence and the crow deliberately take a random orbit to protect its food. This behavior is simulated by applying a random motion in the CSA [24].

The concepts of crow search algorithm [25]:

a) Crows can live in the pattern of flocks.
b) Crows remember the secret places location.
c) Crows often follow each other to steal.
d) Crows preserve their hiding places from a prospect thievery

Figure 1 resent pseudo code for the algorithm of crow search.

Crow search algorithm
Randomly initialize the position of N crows in the search space
Evaluate the position of the crows
Initialize the memory of each crow
while iter <Maxiter
for i = 1 : N (all N crows of the flock)
Randomly choose one of the crows to follow (for example j)
Define an awareness probability
if $r_i \geq AP_j^{iter}$
$x_i^{iter+1} = x_i^{iter} + r_i * fl_i^{iter} * \left(m_j^{iter} - x_i^{iter}\right)$
else
x_i^{iter+1} *a random position of search space*
end if
end for
Check the feasibility of new positions
Evaluate the new position of the crows
Update the memory of crows
end while

Figure 1. The algorithm of crow search pseudo code [25]

3. THE PROPOSED SYSTEM

In this system more than one level is applied to generate the key that is used for encryption, the key is generated using crow which will use the unique features of the person to extract features that is used to generate key. Figure 2 shows the proposed system architecture and algorithm shows (1) the main phases in the proposed key generation algorithm.

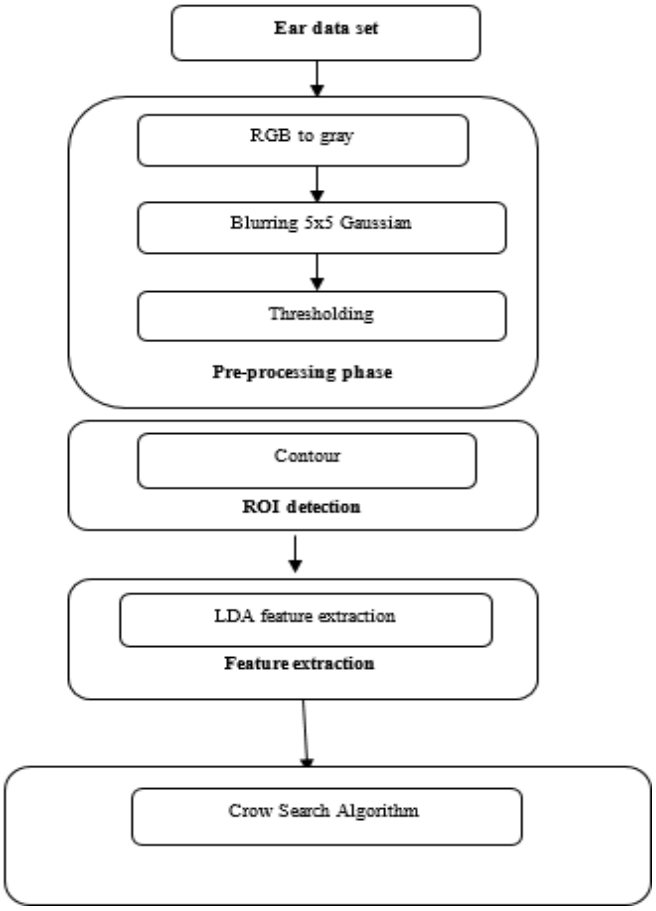

Figure 2. Proposed system architecture

Algorithm 2 proposed key generation algorithm

```
Input: ear image
Output: unique features
Start
Step1: read the input image
Step2: apply pre-processing phase which is consist of three internal steps:
    e)  RGB to gray conversion Using the following equivalence:
        L=0.299R+0.587G+0.114B
    f)  Blurring using Gaussian filter
    g)  Thresholding
Step3: detect the region of interest using contour algorithm.
Step4: extract the features using LDA.
Step5: generate the encryption key using meerkat swarm algorithm.
       End
```

This system consists of five main phases:

3.1. Pre-processing phase

This phase consists of three internal steps which used to prepare the data set for further processing each step in this phase applied for a specific task:

a) RGB to gray conversion: in this step the entered colored image will be transformed into gray scale to decrease the amount of information processed in the system and remove noise.
b) Blurring: this is done via applying the 2D Gaussian filter to enhance the image and reduce the noise within that image.
c) Thresholding: which will convert the image to binary which will be entered to the region of interest extraction using contour which need binary inputs since it senses the black spots.

3.2. Region of interest (ROI) detection phase

The detect part need to be bounded since it is the only part that will need to extracted using feature extraction algorithm, the detection of region of interests done using contour algorithm which will bounded the ear or eye and discard other information on the image.

3.3. Feature extraction phase

This phase aims to extract features from bounded region of interest founded by contour this is done via algorithm LDA.

3.4. Key generation phase

For the ear image 7 keys is generated for each person. To generate these keys, we use crow search algorithm (CSA). In the beginning CSA generate initial random crow positions of keys from features extracted from ears, the generation process done by using logistic map function. The logistic map is evaluated by:

$$xn+1 = r\ xn\ (1-xn) \quad (3)$$

where xn is a number from zero to one representing the current population to the maximum possible population ratio. After generate initial population algorithm compute fitness for population to evaluate the position of crow using fitness function, the strength value can be calculated for each iteration individually. This value is calculated according to of the maximum repeated symbol. The suitability function can be described as the following:

$$F= n + (€ / m) \quad (4)$$

Where
F stands for Fitness Function.
n stands for the entire number of symbols used in key formation.
m stands for the maximum appeared symbol percentage.
€ stands for the ideal percentage for each symbol.

For each crow generate random value ri, compare ri with awareness probability (AP). If ri greater than AP then calculate new position for crow randomly, else calculate new position for crow via levy-flight function. After that chick feasibility of new position, and calculate fitness for new positions. These steps repeated until reach max iteration. After generate best key from extracted feature the proposed system tests this key.

3.5. Test generation keys

The proposed system test kit, produced by CSA (arbitrarily long) can be described as a statistical package composing of seven test developed to test whether a random binary sequence. These tests focus on various non-random types that may be found in a sequence. Several tests can be divided into various sub-tests. These 7 tests are as the following:
a) The Test of Monobit (the frequency)
b) Test of Frequency through a Block.
c) Test of Runs
d) Test of Binary Matrix Rank
e) Test of Discrete Fourier Transform (Spectral)
f) Test of Non-Overlapping Template Matching
g) Test Overlapping Template Matching

4. RESULT DISCUSSION

The proposed system was applied to 46 people, each person has 7 snapshots for ear, each snapshot offers a key to the person. Table 1 shows the result of test keys which are 7 keys for one person, frequency test results in columns, test of frequency within a block results, run test results, binary matrix sequence test results, discrete fourier transform (DFT) test results, non-overlapping template matching test results and matching template matching test results. Two value tests for each test available test result and erfc present error rate function results available. As shown in the Table 1, all values of erfc column in each test is greater than 0.01, that mean the created keys are unartistic.

Table 1. Keys test results

FrequencyTest		FrequencyBlock		RunTest		RankTest		DFT		NonOverling		OverlappingTest	
Tests	Erfc	Tests	erfc	tests	erfc	tests	erfc	Tests	erfc	Tests	erfc	tests	Erfc
0.75	0.530333	37.5	18.75	138	29.01587	5.396498	14.8537	-44.4496	31.42996	0.139519	0.06976	91.15976	45.57988
0.875	0.618718	25.75	12.875	131	9.539423	5.396498	14.8537	-45.2598	32.00349	0.17154	0.08577	87.43411	43.71705
0.5	0.353553	28	14	126	5.298122	5.396498	14.8537	-45.6653	32.29026	0.141806	0.070903	89.06829	44.53415
0.375	0.265165	30.25	15.125	141	36.94812	1.679739	2.316064	-42.4209	29.99611	0.144094	0.072047	90.96091	45.48045
1.625	1.149049	45.75	22.875	130	9.294392	1.679739	2.316064	-46.4764	32.8638	0.093775	0.046888	85.9992	42.9996
0.375	0.265165	30.25	15.125	134	17.16001	1.679739	2.316064	-46.4764	32.8638	0.15553	0.077765	89.23934	44.61967
0.5	0.353553	32	16	139	31.43552	2.037079	2.769148	-46.4764	32.8638	0.102924	0.051462	92.62908	46.31454

5. CONCLUSION

The work has been carried out for hundreds of samples. Each population varies greatly from another. Key length for which test is carried out is 256 bit long. Longer key sequence will also work but time constraint does not permit to check. Encryption and decryption are also performed. This paper proposes the Crow Search Algorithm, and shows its potential to generate Keys from biometric features and obtain the random keys with a smaller number of iterations.

REFERENCES

[1] A. K. Jain, A., Ross, "Introduction to Biometrics. In Handbook of Biometrics," *(Eds), Springer*, 2008

[2] Y. C. Feng, P. C. Yuen, A. K. Jain, "A Hybrid Approach for Face Template Protection," *In Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA*, vol. 6944, pp. 325, 2008.

[3] P. Balakumar, R. Venkatesan, "A Survey on Biometrics-based Cryptographic Key Generation Schemes," *International Journal of Computer Science and Information Technology & Security*, vol. 2, no. 1, pp. 80-85, 2012.

[4] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, pp. 4-20, 2004.

[5] B. Biggio, "Adversarial Pattern Classification," *Doctoral dissertation, University of Cagliari, Cagliari, Italy*, 2010.

[6] G. I. Davida, Y. Frankel, B. J. Matt, "On Enabling Secure Applications through Off-Line Biometric Identification," *In Proceedings of the IEEE Symposium on Privacy and Security*, pp. 148-157, 1998.

[7] Y. J. Chang, W. Zhang, T. Chen, "Biometrics-based Cryptographic Key Generation," *In Multimedia and Expo, ICME'04. 2004 IEEE International Conference*, vol. 3, pp. 2203-2206, 2004.

[8] A. Juels, M. Sudan, "A fuzzy vault scheme," *In Proc. IEEE Int. Symp. Information Theory, IEEE Press*, pp. 408, 2002.

[9] Y. Dodis, L. Reyzin, A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *In Proceedings of the Eurocrypt 2004*, pp. 523-540, 2004

[10] Askarzadeh, A., "Capacitor placement in distribution systems for power loss reduction and voltage improvement: a new methodology," *IET Generation, Transmission & Distribution*, vol. 10, no. 14, pp. 3631–3638, 2016.

[11] Y. J. Chang, W. Zhang, T. Chen, "Biometrics-based Cryptographic Key Generation," *In Multimedia and Expo, ICME'04. 2004 IEEE International Conference*, vol. 3, pp. 2203-2206, 2004.
[12] L. Wu, X. Liu, S. Yuan, P. Xiao, "A Novel Key Generation Cryptosystem based on Face Features," *In Signal Processing (ICSP) 2010 IEEE 10th International Conference on*, pp. 1675-1678, 2010.
[13] Feng Hao, Ross Anderson and John Daugman, "Combining Crypto with Biometrics Effectively", *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081 - 1088, 2006.
[14] Beng.A, Jin Teoh and Kar-Ann Toh, "Secure biometrickey generation with biometric helper," *in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications*, pp. 2145-2150, 2008.
[15] S.Mishra and S.Bali, "Public key cryptography using genetic algorithm," *International Journal of Recent Technology and Engineering*, vol. 2, no. 2, pp. 150-154, 2013.
[16] S.Jhajharia, S.Mishra and S.Bali, "Public key cryptography using particle swarm optimization and genetic algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 832-839, 2013.
[17] F.S.A.-Mouti, M.E.Elhawary, "Overview of artificial bee colony algorithm and its applications," *IEEE International Conference–System Conference*, pp. 1-6, 2013.
[18] Sanaul Hoque, Michael Fairhurst and Gareth Howells, "Evaluating Biometric Encryption Key Generation Using Handwritten Signatures", *in Proceedings of the 2008 Bio-inspired, Learning and Intelligent Systems for Security*, pp.17-22, 2008.
[19] Beng.A, Jin Teoh and Kar-Ann Toh, "Secure biometric-key generation with biometric helper", *in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications*, pp. 2145-2150, 2008.
[20] Ahmed T. Sadiq Al-Obaidi, Hasanen S. Abdullah, Zied O. Ahmed, "Meerkat Clan Algorithm: A New Swarm Intelligence Algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, pp. 354-360, 2018.
[21] Primitivo Díaz, Erik Cuevas, "An Improved Crow Search Algorithm Applied to Energy Problems", *Energies*, vol. 11, no. 571, 2018.
[22] Askarzadeh, A., "Capacitor placement in distribution systems for power loss reduction and voltage improvement: a new methodology" *IET Generation, Transmission & Distribution*, vol. 10, no. 14, pp. 3631–3638, 2016.
[23] Emery, N. J., & Clayton, N. S., "The Mentality of Crows: Convergent Evolution of Intelligence in Corvids and Apes," *Science*, vol. 306, no. 5703, 2004.
[24] M. K. Marichelvam, K. Manivannan, M. Geetha, "Solving Single Machine Scheduling Problems using an Improved Crow Search Algorithm," *International Journal of Engineering Technology Science and Research IJETSR*, vol. 3, no. 12, 2016.
[25] Askarzadeh, A., "A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm," *Computers and Structures*, vol. 169, no. 1, pp. 1-12, 2016.