Secure Electronic Voting System using Swarm Intelligence

Manar Muwafaq Rasheed
Middle Technical University /Institute of Administration /Rusafa
manar.muafak@yahoo.com

Abstract: One of the important systems for society today is the electronic voting system. All the people around the world are looking for transparency and integrity, and they afraid of voting fraud. Electronic voting system is looking for confirming the true identity of a person. Fingerprint identification may be preferred over traditional methods (e.g. passwords, smart-cards) because its information is virtually impossible to steal. This paper introduces secure election system depending on swarm intelligence techniques, especially PSO and firefly algorithms. The proposed system is successful within 500 iterations for PSO to find best features for fingerprint. Best steganographic positions are found by firefly algorithm. PSO has been reduced the time for features extraction of one fingerprint from (1.1 sec) to (0.36 sec). Firefly algorithm has been raised the PSNR of the stegocovers up to (66.246-69.447)dB. The percentage matching of all bands at receiver side is 100%.

Keywords: Secure electronic voting system, Biometrics, Fingerprint identification, Swarm intelligence, Steganography, PSO, Firefly algorithm.

1. Introduction

There are several identification verification schemes that exist today but the most accurate identification schemes are in the area of biometrics. Some examples of identifying biometric characteristics are fingerprints, hand geometry, retina and iris patterns, facial geometry, and signature and voice recognition[1]. A biometrics system is a pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user [2].

A good biometric system must ensure that (1) the biometric information comes from a live person at the time of verification, and (2) the biometric information matches the master biometric data on file. However, a big threat for biometric authentication is still compromise of a user’s biometric information [3]. The reason is that many platforms and biometric systems are used without their untrustworthiness being detected. If an impostor is able to access a user’s biometric information, he or she can then replay this
information to a matching algorithm used for user authentication, and be accepted as a valid user, given that the matching algorithm is not able to recognize the origin of the biometric information [4].

Usually the aim of communicants is merely to transmit a message as quickly, accurately and cheaply as possible. There are, however, a number of situations where the information is confidential and where an interceptor might be able to benefit immensely from the knowledge gained by monitoring the information circuit [5]. The interceptor might also be able to modify the transmitted messages[6]. This is very critical situation especially in elections. There are several ways to solve this problem, one of these solutions is through the use of steganography.

One important direction that has been explored widely in last decade is the concept of swarm intelligence to develop various artificial systems [7]. These systems might be used in electronic voting systems.

This paper relates concepts of biometrics, secure system, swarm intelligence, and steganography with each other in building a proposed electronic voting system.

2. Swarm Intelligence

Swarm Intelligence (SI) is part of artificial intelligence. In practice, the main aim of A.I during the last four decades has been to develop “Intelligent machine” with the capabilities for solving complex task similar to human beings. It based on the study of collective behavior in decentralized and self-organized systems. The idea of SI comes from systems found in nature, including ant colonies, bird flocking and animal herding that can be effectively applied to computationally intelligent system. SI systems are typically made up of a population of agents interacting locally with one another and with their environment and local interactions between such nodes often lead to the emergence of a global behavior[8][9].

2.1 Particle Swarm Optimization

The particle swarm optimization algorithm (PSOA), which was first introduced by Kennedy and Eberhart in 1995 [10]. The basic PSO model consists of a swarm of particles, which are initialized with a population of random candidate solutions. They move iteratively through the d-dimension problem space to search for the new solutions, where the fitness, $f$, can be calculated as the certain qualities measure.

Each particle has a position represented by a position-vector $x_i$ (i is the index of the particle), and a velocity represented by a velocity-vector $v_i$. Each particle remembers its own best position so far in a vector $i$-th, and its d-dimensional value is $p_{best}(p_{id})$.

The best position-vector among the swarm so far is then stored in the vector $i$-th, and its d-th dimensional value is $g_{best}(p_{gd})$. During the iteration time $t$, the update of the velocity ($v_{id}$) from the previous velocity to the new velocity is determined by Eq. (1). The new position ($x_{id}$) is then determined by the sum of the previous position and the new velocity by Eq. (2).

$$V(id+1) = w*v(id) + c1*r1* (pgd-x(id)) +c2 * r2 * (p(id) -x(id))... (1)$$
$$X(id+1) = x(id) + v(id+1)...................................... (2)$$
where \( i = 1, 2, \ldots, N \); \( w \) is the inertia weight, \( r_1 \) and \( r_2 \) are the random numbers, which are used to maintain the diversity of the population, and are uniformly distributed in the interval \([0, 1]\) for the \( d \)-th dimension of the \( i \)-th particle. \( c_1 \) is a positive constant, called coefficient of the self recognition component; \( c_2 \) is a positive constant, called coefficient of the social component. The general basic algorithm for the Particle Swarm Optimization can be described in algorithm (1) [11].

**Algorithm (1) PSO Algorithm**

*Input*: Initialize the algorithm parameters \((c_1, c_2, w, v_{max}, Swarm\_Size, Max\_Iter, r_1, r_2)\).

*Output*: The optimization having the highest fitness as found by PSO.

1. Randomly generate the initial particles and velocities to form a swarm.
2. Calculate the fitness function of each of the particles.
3. If the current position of the particle is better than the previous history, update the particles to indicate this fact.
4. Find the best particle of the swarm. Update the positions of the particles by using equations (1) and (2).
5. If the maximum number of iterations has exceeded or high fitness is found, then go to step 6 or else go to step 2.
6. Copy the best value and exit.

### 2.2 Firefly Algorithm

The Firefly algorithm was developed by Xin-She Yang and it is based on idealized behavior of the flashing characteristics of fireflies. For simplicity, we can summarize these flashing characteristics as the following three rules [12]: All fireflies are unisex, so that one firefly is attracted to other fireflies regardless of their sex. Attractiveness is proportional to their brightness, thus for any two flashing fireflies, the less bright one will move towards the brighter one. The attractiveness is proportional to the brightness and they both decrease as their distance increases. If no one is brighter than a particular firefly, it will move randomly. The brightness of a firefly is affected or determined by the landscape of the objective function to be optimized [13]. Based on these three rules, the basic steps of the firefly algorithm (FA) can be summarized as shown in algorithm (2) [14].
Algorithm (2) Firefly Algorithm

Begin

Initialize algorithm parameters:
- $\text{Max Gen}$: the maximal number of generations
- $\gamma$: the light absorption coefficient
- $r$: the particular distance from the light source
- $d$: the domain space

Define the objective function of $f(x)$, where $x=(x_1, \ldots, x_d)^T$

Generate the initial population of fireflies or $x_i$ ($i=1, 2, \ldots, n$)

Determine the light intensity of $l_i$ at $x_i$ via $f(x_i)$

While ($t < \text{Max Gen}$)

For $i = 1$ to $n$ (all $n$ fireflies)
For $j=1$ to $n$ (n fireflies)

if ($l_j > l_i$), move firefly $i$ towards $j$. end if

Attractiveness varies with distance $r$ via $\text{Exp}[-\gamma r^2]$

Evaluate new solutions and update light intensity;

End for $j$
End for $i$

Rank the fireflies and find the current best;

End while

Post process results and Visualization.

End

3. The Proposed Secure Electronic Voting System

The proposed system consists of three stages as shown in figure (1). These stages are described in the following subsections.
3.1 Creation of Users Database stage

The first stage in the proposed system is the creation of users database as shown in block diagram in figure (2).
6

Feature Extraction by PSO

One User fingerprint features

Feature 1 From LL
Feature 2 From LH
Feature 3 From HL
Feature 4 From HH

Figure (2) Block Diagram of creation Database of Users in The Proposed System

3.1.1 User ID Information

User identification (ID), information consists of: The (ID) field is a unique number for each person, the features field is four features from the user's fingerprint, name field is the name of the user, age field is the age of the user, address field is the address of the user, and phone field is the phone number of the user.
3.1.2 Image Preprocessing

After fingerprint image is taken from the user, the image is enhanced and prepared by doing the following processes sequentially:

1- Object Finder of Fingerprint Image: removing the non-useful areas from fingerprint image.
2- Convert Fingerprint Image to Gray level Image: the colored fingerprint image is transformed to gray-level image using the intensity relationship depending on eq.(3):
   \[ \text{Intensity} = (0.2126 \times \text{Red} + 0.7152 \times \text{Green} + 0.0722 \times \text{Blue}) \] ……………..(3)
3- Image Smoothing: Median filter is used for smoothing. Median filtering reduces noise without blurring edges and other sharp details depending on [15].
4- Image Sharpening: is used for highlighting fine details or enhancing the details of a fingerprint image. Laplacian is the technique used for sharpening depending on [16].

3.1.3 Multiwavelet Transform of Processed Fingerprint Image

Two-dimensional discrete wavelet transform (2-D DWT) [17] decomposes a gray-level fingerprint image into one average component sub-band and three detail component sub-bands. The first sub-band is LL and contains average components, second sub-band is LH and contains vertical edges, third sub-band is HL and contains horizontal edges and HH sub-band and contains diagonal edges.

3.1.4 Feature Extraction using PSO

PSO algorithm (Algorithm 1) is applied to the four subbands of the wavelet transformed image. The fitness function is evaluated for each location in the image and calculated by using statistical calculations. These calculations are X-position, Y-position, Mean, and Variance. X-position and Y-position refer to the two dimensional locations of the coefficient in the subband image. where: \( x(i) \) is the datum in specific position, and \( M \) is the number of location in the subband image. The bird (particle) has the following information: ( \( f(x) \) : fitness of the current position of the bird; \( f(\text{gbest}) \) : best fitness of the position in the search space; \( f(\text{xbest}) \) : best fitness of the neighbors \( f(x) \); \( L_x \) means current position of the fitness bird; \( L_{gbest} \) : position of the best fitness in the search space; \( L_{xbest} \) : position of the best fitness of the neighbor \( f(x) \); \( \alpha, \beta \) : Acceleration parameters (are cognitive and social parameters that are bounded between 0 and 2); \( \text{rand1} \& \text{rand2} \) are the random numbers distributed uniformly in \([0, 1]\); \( D \): maximum number of iteration). Four features (values) are extracted by PSO algorithm according to four sub bands (LL, LH, HL, HH), i.e. PSO is applied four times. The applied PSO is clarified in block diagram of figure (3). Flying bird (particle) on the search space (sub image) starts from the center of it to find optimal solution (location) by iteration method. When a particle finds a location that is better than any previously found locations, then it updates it as the new best current location for particle (particle updates its own velocity and its position using Eq.(4) and Eq.(5) respectively).

- \( f_i(t+1) = f(x) + \alpha \times \text{rand1} \times (L_{gbest} - L_x) + \beta \times \text{rand2} \times (L_{xbest} - L_x) \)……..(4)
- \( L_{x_i}(t+1) = L_x + f_i(t+1) \) ……………………………………..(5)

This is the first feature extracted from LL subband. This process is applied on three other subbands (LH, HL, HH), therefore four features are extracted from fingerprint image.
Input 4 sub image : ( LL,LH,HL,HH), Initialize c1,c2, rand1, rand2, max iteration D, feature W

For each sub image do

Set $D=1$, $W=0$

Put particle in the center position of each image

Calculate the fitness value

If

yes

$f(x_{\text{best}}) = f(x)$ and $L_{\text{best}} = L_x$

if

no

$f(g_{\text{best}}) = f(x)$ and $L_{g_{\text{best}}} = L_x$

$w = w + \text{value (g_{best})}$

$P = w / \text{number of g_{best}}$

If $D <= 500$ ?

yes

Averaged Feature = $p$

no

update particle position using Eq. (5)

update particle velocity using Eq. (4)

Figure(3) Block Diagram of PSO algorithm for Feature Extraction
3.1.5 Creation of Database Templates

This is the last step in this stage, the proposed system will create database templates to save the four features that are extracted from each fingerprint image temporarily. The proposed system relays on the matching operation for granting the authentication operation. Two authenticate operations are called ("one to one" and "one to many") are used. In both types of matching, if the matching ratio between (database LL feature and temporary LL feature) is lower than 98% the person is unauthorized and if it is equal or greater than 98% then another comparison between (database LH, HL, HH features and temporary LH, HL, HH features) is done. If the result of second comparison is equal or greater than 90% than the person is authorized otherwise the person is unauthorized.

3.2 Transmitter stage

The block diagram of transmitter stage is shown in figure (4).
3.2.1 Initial Steps of Transmitter Stage

Initial steps (input fingerprint image, object finder, convert to gray level, filtering, multiwavelet transform, and feature extraction) of this stage are similar to the operations of the steps in creation user database stage described in (3.1) subsection except that the four features that have been obtained from the PSO algorithm will not be stored in the database, but they are sent over the Internet channel to the receiver with the ID and opinion.

3.2.2 Steganography Using Firefly Algorithm

The Internet does not use secure links, thus information (features, ID, opinion) may be corrupted or eavesdropped. Therefore, steganography must take place before transmission. Figure (5) shows the block diagram of hiding features inside cover image using firefly algorithm with LSB techniques. Figure (6) describes firefly algorithm in finding best hiding locations in cover image.
Figure (5) Block Diagram of Hiding Features Inside Cover Image using Firefly Algorithm with LSB Technique

Start

Input Cover Image

Apply Firefly Algorithm on Cover Image

Select Locations with Pixel Values

Split each Value to R-G-B

Convert Blue Color to Binary Form

Input Features, Opinions

Convert Features, Opinion to Binary form

Apply LSB to Blue Color According to Features bits

Reconstruct Pixel Value With New Blue Color Value

Reconstruct Cover image with new pixel Value

If Features and Opinion are Finished

yes

Get Stego Cover

End

Start

Input cover image, (m) max iterations=15, (n) no. of secret features bits =432
Figure (6) Block Diagram of Firefly Algorithm For Finding Best Hiding Locations in Cover Image

1. Calculate the distance between the brightest and other pixels.
2. Determine brightest fireflies, highest pixels values.
3. Calculate the attractiveness between each pixel and brightest.
4. Calculate the movement (x) of Pixels to the brightest ones.
5. Rank (x) using quick sort.
6. Rank pixels according to (x).
7. If $M \leq 15$, then take (n) sorted pixel (values and locations).
8. $m = m + 1$.
9. End.
3.3 Receiver Stage:

The block diagram of receiver stage for the proposed system is shown in figure (7).

Figure (7) Block Diagram of the Receiver Stage in the Proposed System

At receiver stage; stego image is received, and features with opinion are extracted and matched. The first step in block diagram of figure (7) is applying firefly algorithm on stego image, in order to find hiding locations (pixels). The blue color in specified pixels is splitted and converted to binary form. Hence, the secret features, ID, and opinion are extracted using LSB technique (taking last bits from specified binary values). The (one-to-one) matching between extracted features and database features is not done without ID being recognized in database.
In (1:1 and 1:many) matching, if the matching ratio between (database LL feature and temporary LL feature) is lower than 98% the person is unauthorized and if it is equal or greater than 98% then another comparison between (database LH, HL, HH features and temporary LH, HL, HH features) is done. If the result of second comparison is equal or greater than 90% than the person is authorized otherwise the person is unauthorized.

4. Results

The experimental results are tested with (300) fingerprints images. These samples are taken from different students at the Institute of computer Science at Sulaimaniya city using M2sys device. Also different test images are used as cover images in these results.

4.1 Results of Preprocessing Fingerprint Image

The results of preprocessing fingerprint image are shown in figure (8).

![Figure (8) Results of preprocessing Fingerprint Image](image)

(a) Original Fingerprint Image  (b) After Object Finder  (c) After Converting to Gray Level  (d) After Smoothing  (e) After Sharpening

4.2 Results of Extracting Features Using PSO

PSO algorithm is applied with (500) iterations for each subband. The random values in equation (1) are stored in both transmitter and receiver sides for convenience. The best locations were located by PSO algorithm are shown in figure (9).

![Figure (9) Best locations Visited by PSO Algorithm](image)
Relation between Values and Locations Selected by PSO Algorithm is shown in figure (10).

![Relation Between Values and Locations Selected by PSO Algorithm](image1)

**Figure (10) Relation Between Values and Locations Selected by PSO Algorithm**

### 4.3 Results of Firefly Algorithm

Figure (11) shows the relationship between the locations that are selected by the firefly algorithm and the values of these locations.

![Relation Between Values and Locations Selected by Firefly Algorithm](image2)

**Figure (11) Relation Between Values and Locations Selected by Firefly Algorithm**

Figure (12) shows (3) cover images with and without the location that are selected by the firefly algorithm. Note that the selected Locations are specified by green color.

![Cover Images](image3)
Figure (12) Cover Images with and without Selected Locations by Firefly Algorithm

The quality metrics of stego images are shown in table (1).

| Image  | MSE      | PSNR    |
|--------|----------|---------|
| Image A | 0.007    | 69.447  |
| Image B | 1.543E-02| 66.246  |
| Image C | 0.008    | 68.907  |

4.4 Results of Receiver Stage

The four extracted features are matched (1-to-1) with database created at subsection (3.1). This operation process is shown in table (3).

| Extracted Features | Extra ID  |
|--------------------|-----------|
| LL                 | 162.8842315369 |
| HL                 | 18.5988023952  |
| LH                 | 38.2275449101  |
| HH                 | 18.8363273453  |
|                   | 13          |
5. Evaluation
Table (5) shows that there are different factors to evaluate the proposed systems depending on results of shown in subsection (3).

| LL Matching Ratio | Other Matching Ratio | Matching |
|-------------------|----------------------|----------|
| 100%              | 100%                 | Yes      |

Table (5) An Evaluation of The Proposed System

| Time required to extract features | Time required to LSB hiding | MSE of same stegocover | PSNR of same Stegocover | Matching of extracted features of (300) users | Robustness of hiding |
|----------------------------------|-----------------------------|------------------------|-------------------------|---------------------------------------------|---------------------|
| 52 Sec                           | 40 Sec                      | 0.007                  | 69.447                  | 100%                                        | Conversion test: fail |

Table (6) shows the proposed system performance depending on:(FAR, FRR, and CAR).

| FAR | FRR | CVR% | FAR | FRR | CVR% |
|-----|-----|------|-----|-----|------|
| LL Band | LL Band | LL Band | ALL Bands | ALL Bands | ALL Bands |
| 0.00 | 0.02 | 98   | 0.00 | 0.00 | 100  |

6. Conclusion
Conclusions that can be inferred from this work are specified below:

1. The advantages of using PSO for features extracting are:
   a. Obtaining best features from fingerprint as clarified in figure (10) and table (3).
   b. Minimizing the time required for processing as clarified in table (4).

2. The advantages of using firefly for LSB steganography are:
   a. Obtaining best locations for hiding as shown in figure (11).
   b. Obtaining high security for the proposed system.
References

[1] Ziyad Tariq Mustafa Al-Ta’i and Omer Younis Abd Al-Hameed, "Comparison between PSO and Firefly Algorithms in Fingerprint Authentication", International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 1, July 2013.

[2] Nor Farizan Bintizakaria, "Implementation Of Fingerprint biometric Template System In Embedded Software Design ", Msc. Thesis, Faculty of Electrical Engineering, University of Malaysia, May 2006.

[3] J.D. Woodward, "Biometrics: Privacy’s Foe or Privacy’s Friend", In the Proceedings of the IEEE, Special Issue on Automated Biometrics, Vol. 85, No. 9, pp.1480, 1997.

[4] Liquin Chen, Siani Pearson, Athanasios Vamvakas, "A Trusted Biometric System", Report from Trusted E-Services Laboratory, HP Laboratories Bristol, Filton Road, Stoke Gifford, Bristol, UK, July 2002.

[5] Ziyad Tariq Mustafa Al-Ta’i, "Simulation of New Covert Audio Cryptographic Model", 3rd International Conference on Machine Learning and Computing (ICMLC 2011), Singapore, 26-28 February 2011.

[6] Ziyad Tariq Mustafa Al-Ta’i, "Development of Multilayer New Covert Audio Cryptographic Model", International Journal of Machine Learning and Computing, Vol. 1, No. 2, June 2011.

[7] Lučić Panta and Teodorović Dušan, "Modeling Transportation Problems Using Concepts of Swarm Intelligence and Soft Computing", Ph.D Thesis in Civil Engineering, Virginia Polytechnic Institute and State University, USA, 2002.

[8] Bonabeau, Dorigo M., and Theraulaz G., "Swarm Intelligence: From Natural to Artificial Systems", book from Oxford University Press, 1999.

[9] Teodorovic Dusan. "Transport Modeling by Multi-agent system: A swarm Intelligence approach", Transportation planning and Technology, Vol. 26, No.4, PP.289-213, 2003

[10] Kennedy J. and Eberhart R. C., "Particle Swarm Optimization", Proceedings of the 1995 IEEE International Conference on Neural Networks, volume 4, PP: 1942–1948, Australia, IEEE Service Center, 1995.

[11] Mudhafar A. Salim et al 2020 J. Phys.: Conf. Ser. 1664 012105.

[12] Ismail Khalil Ali, " Intelligent Cryptanalysis Tool Using Particle Swarm Optimization", Ph.D.Thesis, Univercity of Technology, Department of Computer Science, Iraq, 2009.

[13] Salam Hussein Ewaid et al 2020 J. Phys.: Conf. Ser. 1664 012143.

[14] Sh. M. Farahani, A. A. Abshouri, B. Nasiri, and M. R. Meybodi, " A Gaussian Firefly Algorithm", International Journal of Machine Learning and Computing, December 2011.

[15] Xin-She Yang, "Nature-Inspired Metaheuristic Algorithms" Book from Luniver Press, united kingdom, 2008.

[16] Ewaid, S.H.; Abed, S.A.; Al-Ansari, N.; Salih, R.M. Development and Evaluation of a Water Quality Index for the Iraqi Rivers. Hydrology 2020, 7, 67.

[17] Ewaid, S.H., Al-Farahani, B.F., Abed, S.A. & Al-Ansari, N. (2020). Modeling of trihalomethane compounds formation in Baghdad water supply network. Scientific Review Engineering and Environmental Sciences, 29 (2), 136-144. doi: 10.22630/PNIKS.2020.29.2.12.

[18] Salam Hussein Ewaid et al 2021 IOP Conf. Ser.: Earth Environ. Sci. 722 012008
[19] Ahmed Alaa Kandoh and Salwan Ali Abed 2021 IOP Conf. Ser.: Earth Environ. Sci. 790 012034
[20] Ahmed Alaa Kandoh et al 2021 IOP Conf. Ser.: Earth Environ. Sci. 790 012073
[21] N. Chai-ead, P. Aungkulanon, and P. Luangpaiboon, "Bees and Firefly Algorithms for Noisy Non-Linear Optimisation Problems", Proceeding of the international Multi Conference of Engineers and Computer Scientists, 2011.
[22] Ghazali Bin Sulong," Design and Development of an automatic Fingerprint Verification System", Project Report Faculty science Computer and information system, University of technology Malaysia, 2005.
[23] Ahmed Sabah Al-Jasimee et al 2020 J. Phys.: Conf. Ser. 1664 012141.
[24] Rafael C. Gonzalez, and Richard E. Woods., "Digital image processing", Second edition, book from Prentice Hall, 2002.
[25] Salam Hussein Ewaid et al 2021 IOP Conf. Ser.: Earth Environ. Sci. 790 012075
[26] S.Audithan, RM. Chandrasekaran, " Document Text Extraction from Document Images Using Haar Discrete Wavelet Transform" , European Journal of scientific Research, Internet survey, http://www.eurojournals.com/ ejsr.htm, 2009.
[27] Anil K. Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle, " An Identity Authentication System Using Fingerprints", Proceedings of the IEEE, VOL. 85, NO. 9, September 1997.
[28] A.Wanns Alghurabi, F., & K. Jwad, S. (2019). Separation, preconcentration, extraction and spectrophotometric determination of Mn(VII) from Acidic Aqueous medium. Al-Qadisiyah Journal Of Pure Science, 24(1), 31 - 36.
[29] Ali Abed , S., & A. Salim, M. (2019). THE FIRST OBSERVATION OF THE BANK MYNA ACRIDOTHERES GINGINIANUS (LATHAM, 1790) (FAMILY: STURNIDAE, CLASS: AVES) IN THE WILD IN IRAQ. Al-Qadisiyah Journal Of Pure Science, 24(1), 45 - 48.
[30] Abdul-Hamza, H. kadhum, & Mohammed, G. J. (2019). The inhibitory effect of some nanoparticles on biofilm formation of Streptococcus agalactiae. Al-Qadisiyah Journal Of Pure Science, 24(2).