International Journal of Current Engineering and Technology
©2017 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Secure Online Voting using Steganography and Biometrics

Marwa K. Alhasnawi* **and Ali S. Alkhalid**

Electrical Engineering Technical College, Middle Technical University-Iraq

Accepted 25 May 2017, Available online 03 June 2017, **Vol.7, No.3 (June 2017)**

Abstract

The fundamental knowledge beyond electronic voting system is to confirm integrity and reliability of specific mechanisms for addressing issues of security, privacy and accountability, which results due to the rapid development of information technology field over time and the traditional election procedures, which cannot satisfy all of voter's demands. The primary goal of every voting system is to increase the participation of voters in addition to online voting are simple, attractive and easy to use. It reduces manual efforts and bulk of information can be handled easily. Furthermore, the development of technology needs to increase the reliability so that only the authorized persons are allowed to cast their votes and ensure that the voting results will not change. The necessity to find a technique ensures the safety of election led to presents a novel approach to provide secure mobile voting based on Biometrics in conjunction with elliptic curve cryptography and steganography.

Keywords: *Biometrics, Elliptic Curve Cryptography, Steganography.*

1. Introduction

Voting is a main part of the democratic operation. The electorate makes an expresses or decision an opinion that is accepted by everybody. Ensuring the integrity of elections is the most important factor to succeed the democracy process. Therefore, the electronic voting system must be secure and robust against a variety of fraudulent behaviors, and should be transparent and comprehensible. If the security of the system is done well, electronic voting can be a great improvement to the paper traditional systems. For this reason, there is a need for additional layer of security to avoid the risk that may happen in such a system. One method to ensure the security and the integrity of the voting process is using the biometrics for identification. Moreover, using crypto_stego system in the E-voting can reduce the risk of transmitting the secret data over insecure wireless medium, where these data can be attacked or hacked (Humphreys, J. B., 1961). (L. Rura *et al*, 2011), suggested the implementation of a secure electronic voting system with a combination of cryptography and steganography in java. Visual cryptography offers less computational assessment measurements because of their complex cryptographic mechanisms and can be considered as a reliable and helpful tool for security assurance. (A.K Vishwakarma *et al*, 2011), suggested a scheme based on the face and voice recognition together for describing the authentication. This demands the physically show up of the voter in order to complete the authentication process. Because it is impossible for two persons to have the same face and the same voice, this type of security provides the best authentication to know the identity of the voter. ECC technique (Elliptic Curve Cryptography) and Steganography were used to strength the security over the unsafe channel. The ECC mechanism was applied on the voter's ID as well as voice and face data at first and then hiding it in an image using steganography, after this it's very difficult for the hackers to identify that the image which is supplied over the network includes any information. In case if the hacker discovered the information which was sent after applying this scheme, he cannot understand the information hidden because of ECC encryption mechanism. (M. Vijay *et al*, 2013), proposed an online voting system using face detection and recognition. This system permits the people to cast their votes from any place in the country.

The system used Eigen face algorithm to identify the voter's image then saved it as first matching point while PIN was used to return the saved image from the database to the same recognition algorithm then keep it as another matching point. The recognition algorithm to test the voter's image if it's the same used these two points or not. If the two points were matched then the person can cast his vote. (B.B.Kharmate *et al*, **2015**), proposed a smart E-voting system, which was entirely works on digital data. AES algorithm was used for voter's data encryption process. This system can examine validity and eligibility of the voter, the inactive votes and illegal user was stayed out of the system.

*Corresponding author: **Marwa K. Alhasnawi**

This paper introduces a practicable method for secure online voting system. Initially, fingerprint feature will extracted using the Particle Swarm Optimization (PSO) algorithm. Then this feature will encrypt together with the Personal Identification Number (PIN) and the Candidate Number using a symmetric encryption algorithm, which is the Elliptic Curve Cryptography (ECC) algorithm. Finally, multiple chaotic logistic maps are used to generate a random hiding locations and the Least Significant Bit technique is used for hiding the encrypted voter's information inside a cover image to produce a stego image, which is sent over the insecure channel.

2. Fingerprint Feature Extraction

Feature extraction can be defined as the process of generating features from images in order to use it in another processing task. The benefit of extracting features from an image is that when the input to any algorithm is very large, the processing of data will take very long time besides it consumes large resource from the computer. The solution is converting the data of the image to a simplest form by extracting specific feature from it (M. M. JAZZAR, 2010).

There are several algorithms that may be used in the process of feature extraction, in this work PSO algorithm is used. In comparison PSO with many other optimization algorithms, has the advantage of strong global search, faster convergence rate, few adjustable parameters, simplicity of the algorithm, and ease of implementation (S.TALUKDER, 2011).

PSO is a population based search procedure in which the individuals, called particles, adjust their position to search through the search space. Each particle *Pi* has a position vector $X_i = (X_{i1}, X_{i2} ... X_{ik})$ and a velocity vector $V_i = (V_{i1}, V_{i2} ... V_{ik})$. For each iteration the particles learn from its own previous best position P_{best} and the best position of all the other particles l_{best} in the swarm, updates its velocity and position. The update equation at *(k + 1)-kh* iteration can be written as in Equ. 1 and 2, (Q. Bai, 2010).

$$v_i(k+1) = v_i(k) + c_1 * r_1 * \left(x_{p_{best,i}} - x_i(t)\right) + c_2 * r_2 * \left(x_{L_{best,i}} - x_i(t)\right) \quad (1)$$

$$x_i(k+1) = x_i(k) + v_i(k+1) \quad (2)$$

3. Elliptic curve cryptography

Elliptic Curve Cryptography (ECC) was introduced in 1985 by Neil Koblitz and Victor Miller. Elliptic Curve Cryptographic (ECC) schemes are public key mechanisms that provide the same functionality as RSA schemes (R. L. Rivest, A. Shamir, and L. Adleman, 1978). The mathematical operations of ECC are defined over the elliptic curve as shown in Equation 3.

$$E(a,b): y^2 \equiv x^3 + ax + b \ (mod\ P) \quad (3)$$

3.1. Elliptic curve point addition and doubling

The rules for addition over the elliptic E_P (a,b) are:

1. Let the points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_1 \neq P_2$ be in the elliptic group E_P(a,b), and ∞ is the point at infinity (R. Afreen and S.C. Mehrotra, 2011). Draw a line through the points P_1 and P_2. This line intersects the curve in exactly one other point P_3'. Then P_3 is the reflection of P_3' about x-axis.

Now translate the geometrical intuition into an algebraic formulation of P_3.The slop λ of the line through the points P_1 and P_2 is as follows:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \ (mod\ P) \ if\ P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} \ (mod\ P) \ if\ P_1 = P_2 \end{cases} \quad (4)$$

$$P_1 + P_2 = P_3 = (x_3, y_3) \quad (5)$$

$$x_3 = \lambda^2 - x_1 - x_2 (\,mod\ P) \quad (6)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \ (mod\ P) \quad (7)$$

The addition of two points is shown in Fig. 1.

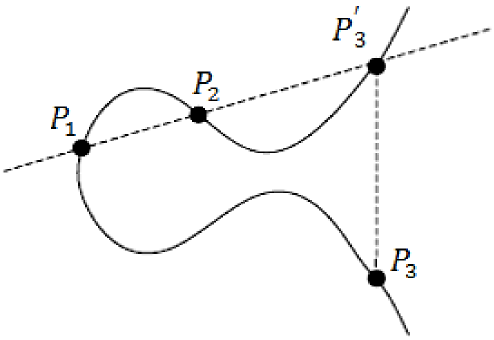


Fig. 1: Addition: $P_3 = P_1 + P_2$.

2. If $x_2 = x_1$ and $y_2 = -y_1$ that is: $P_1 = (x_1, y_1)$, and P_2 $(x_2, y_2) = (x_1, -y_1) = -P_1$, then $P_1 + P_2 = O$.

3. For $P_1 = P_2$, point doubling, draw a tangent line at pointP_1, this line intersects elliptic curve at point P_3'. Then P_3 is the reflection of this point about x-axis as shown in Fig. 2.

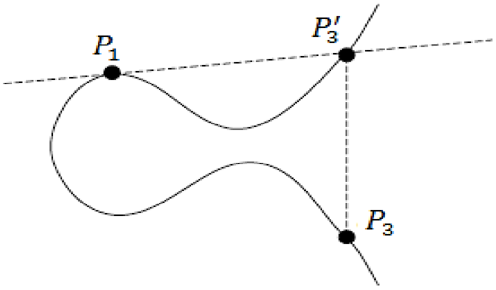


Fig. 2: Doubling: $P_3 = P_1 + P_1$.

3.2. Scalar point multiplication

In point multiplication a point P_1 on the elliptic curve is multiplied with a scalar K using elliptic curve equation to obtain another point P_2 on the same elliptic curve i.e. $KP_1 = P_2$ (M. Brown, *et al*, 2009). Point multiplication is achieved by two basic elliptic curve operations:

- Point addition, adding two point i.e. $P_3 = P_1 + P_2$.
- Point doubling, adding a point P_1 to itself i.e. $P_3 = 2P_1$.

3.3. Encryption and decryption over the elliptic curve

Elliptic curve cryptography can be used to encrypt plaintext messages, m, into cipher texts. The plaintext message m in Fig. 3 is encoded into a point P_m from the finite set of points in the elliptic group, E_P (a,b). The first step consists in choosing a generator point, $G \in E(a,b) \bmod P$. The elliptic group $E_P(a,b)$ and the generator point G are made public.

Each user selects a private key, N_A and computes the public key $P_A = N_A G$. To encrypt the message point P_m for Bob, Alice chooses a random integer K and computes the cipher text pair of points P_C using Bob's public key P_B where the pair of points :

$$P\,c = [(KG), (P_m + KP_B)].$$

After receiving the cipher text pair of points, P_c , Bob multiplies the first point, (KG) with his private key, N_B , and then subtracts the result from the second point in the cipher text pair of points,

$$(P_m + kP_B) - [N_B\,(KG)] = (P_m + KN_B\,G) - [N_B\,(KG)] = P_m.$$

This is the plaintext point, corresponding to the plaintext message m (in numbers). Only Bob, know the private key N_B, which can remove N_B (KG) from the second point of the cipher text pair of points.

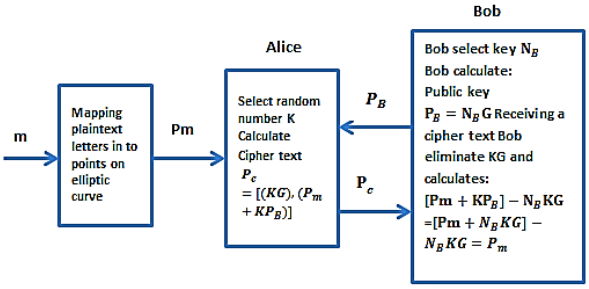

Bob
Alice
m
Mapping plaintext letters in to points on elliptic curve
Pm
Select random number K Calculate Cipher text $P_c = [(KG), (P_m + KP_B)]$
P_B
P_c
Bob select key N_B
Bob calculate:
Public key
$P_B = N_B G$ Receiving a cipher text Bob eliminate KG and calculates:
$[Pm + KP_B] - N_B KG$
$= [Pm + N_B KG] - N_B KG = P_m$

Fig.3: Encryption and Decryption of ECC.

4. Image steganography

Steganography is the art of hiding information plus an effort to hide the presence of the embedded information. It is not proposed to swap cryptography however supplement it. Hiding a message through Steganography approaches decrease the accidental of a message being detected (A. M. B. Witwit, 2001).

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at collection of color pixels so any plain text, cipher text, other images, can be embedded as a bit stream in an image without causing any noticeable changes (A. A. Shejul, U. L. Kulkarni, 2011). Least significant bit is the most popular, simple technique for embedding secret information in a cover image. The procedure is based on a straight substituting the LSBs of the cover image with the message bits (V. K. Sharma, V. Shrivastava, 2012).

5. Chaos theory

Chaos comes from the Greek word 'Χαοs', which meaning a state without predictability or order. A chaotic system is a non-linear, simple, deterministic system, and dynamical that shows totally unexpected behavior and shows randomness. It is used in cryptography for the nature of its features which are high sensitive to initial conditions of the system, randomness and aperiodicity like the long term evolution that results from the deterministic nonlinear systems. Due to these properties; it has been used to create random numbers which can be used then to select hiding locations. With a very small change in their initial values the produced series are totally various (P. Amit, Z. Goseph, 2011; Maqableh, Mahmoud, Mohammad, 2012). There are several chaotic systems, like: Logistic map, Lorenz attractors, Rossler attractors, Henon map and Tent map.

The logistic map is used in this work, is a polynomial mapping, a complex chaotic system, the behavior of logistic map is very simple nonlinear dynamic equations. The 1-dimensional coupled logistic map equation is written as (Maqableh, Mahmoud, Mohammad, 2012):

$$X_{n+1} = RX_n(1 - X_n) \qquad (8)$$

6. The proposed system

The proposed system consists of two parts: Registration part and Voting part as shown in Fig. 4(a) and 4(b).

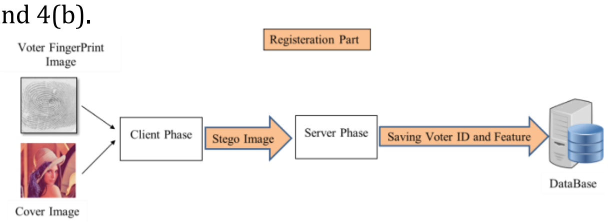


Fig. 4a: The Block diagram of Registration Part.

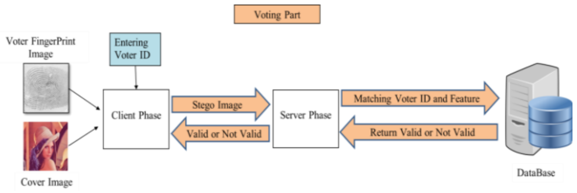


Fig. 4b: The Block diagram of Voting Part.

So, in the registration part, the proposed system used to save the voter PIN, his fingerprint feature and Candidate Number into the server database preparing this information to be used later during the voting day. While in the voting part, the proposed system used to match the voter PIN and his fingerprint feature that taken on the voting day with the information that had been already stored in the server database to distinguish between the people who are allowed to vote from those who are not allowed to vote.

6.1 Fingerprint feature extraction stage

The aim of this stage is to find out the image feature which identifies the person. To apply PSO algorithm on the fingerprint image , it is considered that the pixels in the image represent the particles, the pixel position represent the particle position and pixel value represent the particle velocity , the initial mastermind position will be selected as the center of the image and finally considering the number of iterations as the number of the solutions. The Algorithm1, below will describe this stage in details.

Algorithm 1: Features Extraction using PSO Algorithm.	
Input	The Aspects Image.
output	The feature of fingerprint image (optimal solution).
Step 1	Import Aspect image from the previous algorithm.
Step 2	Getting image size (height and width).
Step 3	Setting up the PSO initial values.
Step 4	Iteration 200 times.
Step 5	○ Calculate the fitness.
Step 6	○ Applying the PSO equations.
Step 7	○ Save the solution in an array.
Step 8	○ Set the solution to be the new best position for the next iteration.
Step 9	○ Shift the pixels in the image according to the position equation.
Step 10	Return to Iteration step 4.
Step 11	Sum all positions in the array and find out the mean of them which represents the fingerprint feature.

6.2 Encryption stage

The goal of this stage is to encrypt the voter information (Fingerprint Feature, PIN and Candidate Number) for more security. The Elliptic Curve algorithm is used in this stage to encrypt this information as shown in the Algorithm 2.

Algorithm 2: Encryption Voter Information Using EC Algorithm.	
Input	Voter Information, Public Values of $E_p(a, b)$, Large number (r), Base point (G) and Private Values (N_A and N_B).
output	Cipher Points represent the encrypted voter information.
Step 1	Enter Voter Information as a plain text.
Step 2	Generate the Elliptic curve points.
Step 3	Mapping the plain text numbers to points lying on Elliptic Curve.
Step 4	Select base point from the Elliptic Curve points.
Step 5	Encrypt each point into two cipher points.
Step 6	Gathering all cipher points of all numbers on the plain text to find out the cipher text.

6.3 Hiding stage

This stage is specifically designed to hide the encrypted information in the selected cover image preparing to send it through unsecure channel, which in this case is the Internet to prevent the security breaching. This stage needs sub stages to achieve its goal. These sub stages are Initializing Two Logistic Maps Sub Stage and Generating Stego Image Sub Stage.

6.3.1 Initializing two logistic maps sub stage

The goal of this sub stage is to generate a secure random numbers, which are used for hiding the information into a cover image. The Logistic chaotic map is suitable for generating these random numbers by giving it the initial condition and control parameter (R, X_n) which can be considered as a secret key. Thus, the proposed system employee two Logistic maps, one generate row numbers and the other generate column numbers. The Algorithm.3 below will describe this sub stage in details.

Algorithm 3: Initialize Two Logistic Maps.	
Input	Initial conditions and control parameters for the two Logistic maps as Secret Key.
Output	Two Period tables (PT1 and PT2), Two vectors (VC1 and VC2).
Step1	Enter Initial conditions and control parameters for the Logistic map representing the Secret Key.
Step2	Generate 40 values from applying Logistic map and stores them in a vector.
Step3	Determine the maximum and minimum values.
Step4	Finding out the increment value based on ((minimum + maximum)/40).
Step5	Generate period table depend on the following steps: ○ The structure of period table consists two fields named From and To. ○ The period table has 40 records only. ○ Filling period table values starts from Zero and ending with maximum value classified by increment value.
Step6	Repeat the above steps using Logistic map with different secret key.
Step7	Assigning the two period tables to be PT1 and PT2.
Step8	Assigning the two vectors to be VC1 and VC2.

6.3.2 Generating stego image sub stage

The goal of this sub stage is to hide the voter information in the cover image, so the system can send the information from the client side to the server side securely. The procedure is to use the hiding locations table, which contains the row and column coordinates in the cover image to hide the voter information.

The technique is starting with separate the color cover image to its three color bands ($V_{Red}, V_{Green}, V_{Blue}$). Then constructing a string named "VoterSt" representing the Fingerprint Image Feature, the voter identity (PIN) and Candidate Number after adjusting the lengths respectively (Set image feature length to a fixed 24 digits, PIN to 10 digits and Candidate Number to 4 digits) to become 38 digits only. Then divide the VoterSt to 19 groups (each group consist of two digits only). According to the location on hiding location table, get the first location and convert the V_{Green} *and* V_{Blue} pixel values to binary representation. After that, convert each group into binary representation. So, starting from the most significant bit (MSB) down to the less significant bit (LSB) the procedure takes the values of each odd bit locations and replace them with the LSB in the V_{Green} pixels in sequence starting from the starting position in V_{Green} matrix that determined by the hiding locations table. This steps will be repeated by taking the values of each even bit locations and replace them with the LSB in the V_{Blue} pixels in sequence starting from the starting position in V_{Blue} matrix that determined by the hiding locations table.

The final step in the algorithm is to gathering the three color bands after hiding the voter information to produce the stego image. The Algorithm 4 below will describe this sub stage in details.

Algorithm 4: Generating Stego Image.	
Input	Fingerprint Image Feature, PIN, Candidate Number, Cover Image and Hiding locations table.
Output	Stego Image.
Step1	Read Cover Image.
Step2	Separating the intensities of each color band of the image and storing them in a separate 2-D matrices naming each matrix with a name derived from its color band name (e.g. V_{red}, V_{green} and V_{blue}).
Step3	Constructing a string named "VoterSt" representing the Image Feature, PIN and the Candidate Number after adjusting the lengths respectively (Set image feature length to a fixed 24 digits , Set PIN length to a fixed 10 digits and Set Candidate Number length to a fixed 4 digits) to become 38 digits only.
Step4	Divide the VoterSt to 19 groups (each group consist of two digits only). According to the location on hiding location table, get the first location and convert V_{green} and V_{blue} pixel values to binary representation.
Step6	For each group (19 group): ▪ Convert the group to binary representation (8 bits only) and name it "SubVoterSt". ▪ Set Counter ← 7. ▪ While Counter ≥ 0 - Replace the LSB in V_{green} with the bit from SubVoterSt depending on Counter position. - Decrement Counter by 1. - Replace the LSB in V_{blue} with the bit from SubVoterSt depending on Counter position. - Get next location from the hiding location table and convert the V_{green} and V_{blue} pixel values to binary representation. - Decrement Counter by 1. ▪ Loop. ▪ Loop.
Step7	Gathering the three color bands to produce the stego image.

The final step in the algorithm is to gathering the three color bands after hiding the voter information to produce the stego image. The Algorithm 4 below will describe this sub stage in details.

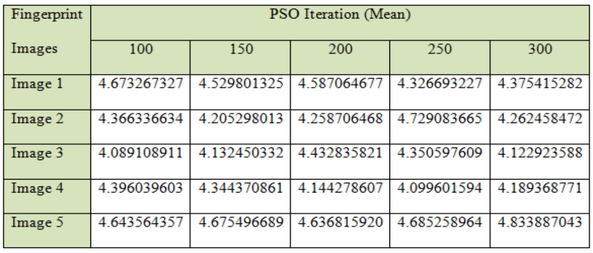
6.4 Extracting information from stego image

Generally, the information extraction from the stego image is done in the server side, which uses reverse steps for hiding information starting from taking the stego image and implementing the secret keys ending with finding out the voter identity (PIN), his fingerprint feature and Candidate Number.

7. Results and discussion

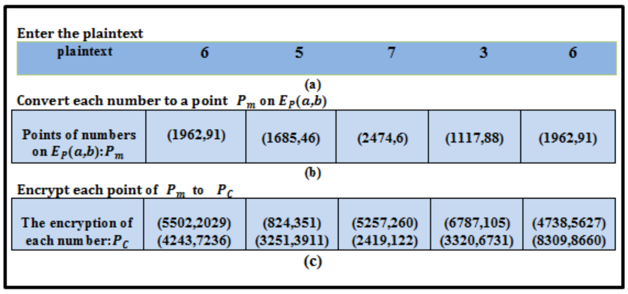
The experiments were done for a number of standard fingerprints images, and color cover image. From table 1, it can be noticed that the extracted features from fingerprint images based on PSO algorithm did not give any intersection between them.

Table 1 PSO feature optimization-using Mean.



Fingerprint Images	PSO Iteration (Mean)				
	100	150	200	250	300
Image 1	4.673267327	4.529801325	4.587064677	4.326693227	4.375415282
Image 2	4.366336634	4.205298013	4.258706468	4.729083665	4.262458472
Image 3	4.089108911	4.132450332	4.432835821	4.350597609	4.122923588
Image 4	4.396039603	4.344370861	4.144278607	4.099601594	4.189368771
Image 5	4.643564357	4.675496689	4.636815920	4.685258964	4.833887043

Fig. (5 and 6) represent the result of the complete system of encryption and decryption a plaintext message "65736". The requirements of the algorithm are the elliptic curve parameters $E_{8831}(3, 45)$, G= (3, 9). Assuming that sender chooses the private key N_A=5, and the receiver choose N_B=21, and large integer r=326.



Enter the plaintext

plaintext	6	5	7	3	6

(a)

Convert each number to a point P_m on $E_P(a,b)$

Points of numbers on $E_P(a,b)$:P_m	(1962,91)	(1685,46)	(2474,6)	(1117,88)	(1962,91)

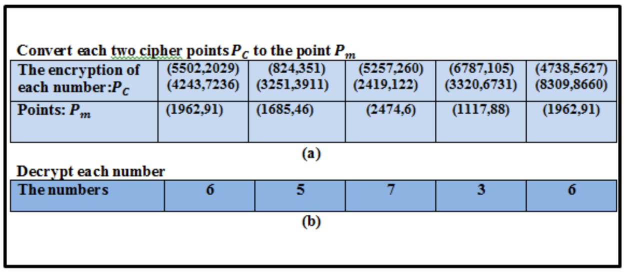
(b)

Encrypt each point of P_m to P_C

The encryption of each number:P_C	(5502,2029) (4243,7236)	(824,351) (3251,3911)	(5257,260) (2419,122)	(6787,105) (3320,6731)	(4738,5627) (8309,8660)

(c)

Fig. 5: Encryption of the plaintext by the sender.



Convert each two cipher points P_C to the point P_m

The encryption of each number:P_C	(5502,2029) (4243,7236)	(824,351) (3251,3911)	(5257,260) (2419,122)	(6787,105) (3320,6731)	(4738,5627) (8309,8660)
Points: P_m	(1962,91)	(1685,46)	(2474,6)	(1117,88)	(1962,91)

(a)

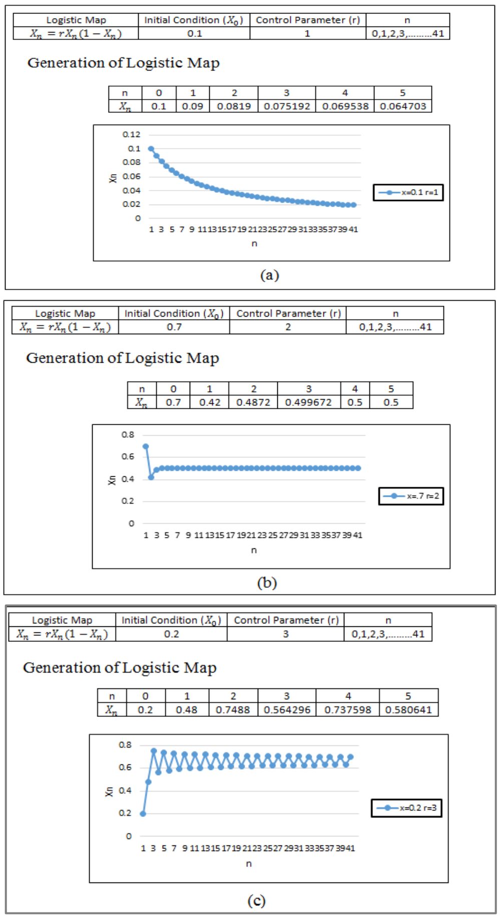
Decrypt each number

The numbers	6	5	7	3	6

(b)

Fig. 6: Decryption of the cipher points by the receiver.

The logistic map is one of the simplest chaotic maps; it is highly sensitive to change in its parameter value, where a different value of the parameter R and X_0 will give quite different locations, as shown in Fig. **7**. This figure shows that R=4 is the best parameter of logistic map and gives more randomness.



Logistic Map	Initial Condition (X_0)	Control Parameter (r)	n
$X_n = rX_n(1-X_n)$	0.1	1	0,1,2,3,.........41

Generation of Logistic Map

n	0	1	2	3	4	5
X_n	0.1	0.09	0.0819	0.075192	0.069538	0.064703

(a)

Logistic Map	Initial Condition (X_0)	Control Parameter (r)	n
$X_n = rX_n(1-X_n)$	0.7	2	0,1,2,3,.........41

Generation of Logistic Map

n	0	1	2	3	4	5
X_n	0.7	0.42	0.4872	0.499672	0.5	0.5

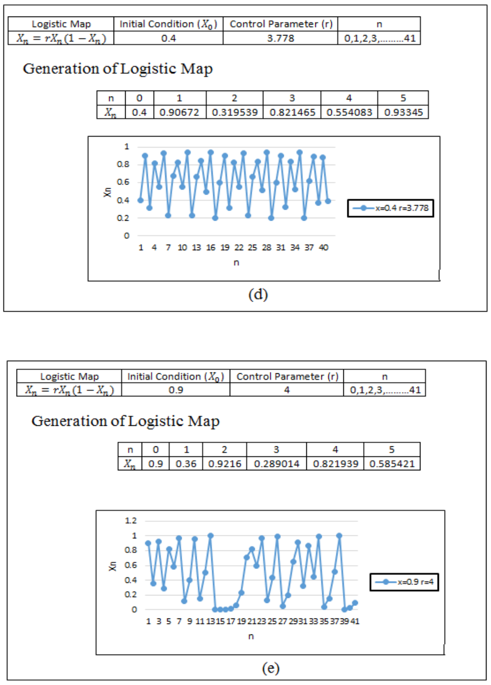
(b)

Logistic Map	Initial Condition (X_0)	Control Parameter (r)	n
$X_n = rX_n(1-X_n)$	0.2	3	0,1,2,3,.........41

Generation of Logistic Map

n	0	1	2	3	4	5
X_n	0.2	0.48	0.7488	0.564296	0.737598	0.580641

(c)



Logistic Map	Initial Condition (X_0)	Control Parameter (r)	n
$X_n = rX_n(1-X_n)$	0.4	3.778	0,1,2,3,.........41

Generation of Logistic Map

n	0	1	2	3	4	5
X_n	0.4	0.90672	0.319539	0.821465	0.554083	0.93345

(d)

Logistic Map	Initial Condition (X_0)	Control Parameter (r)	n
$X_n = rX_n(1-X_n)$	0.9	4	0,1,2,3,.........41

Generation of Logistic Map

n	0	1	2	3	4	5
X_n	0.9	0.36	0.9216	0.289014	0.821939	0.585421

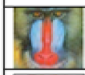
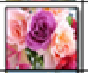
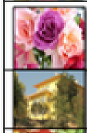
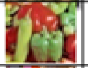
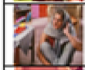
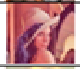
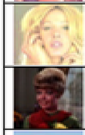
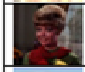
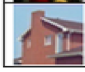
(e)

Fig. 7: The Bifurcation Parameters of Logistic Map.

In Table 2 MSE and PSNR, measurements are applied on the cover image and the stego image to determine the differences between them.

Fig. 8 shows that the correlation between the image pixels in three directions (Horizontal, Vertical and Diagonal) for both covers images and stego images is very high (near to one) which are high intelligibility.

Table. 2: The test results for Multiple - Logistic Maps Embedding Technique.

Secret Image	Initial Condition				Image size	Quality Measures	
(SI)	X0	R	X0	R	(IS)	(MSE)	(PSNR)
	0.2	2.768	0.4	1.843	100×85	0.0026	73.9354
	0.3	4	0.7	3.871	125×93	0.0025	74.1111
	0.8	1.154	0.4	4	165×165	0.0009	78.5010
	0.9	4	0.6	4	75×60	0.0050	71.1090
	0.7	2.33	0.2	2.560	100×100	0.0026	73.9257
	0.6	3.756	0.3	3.987	109×99	0.0074	69.4124
	0.5	3.41	0.6	2.551	130×100	0.0022	74.6462
	0.2	4	0.4	4	80× 80	0.0036	72.5128
	0.6	3.572	0.6	3	185 ×125	0.0010	77.9096

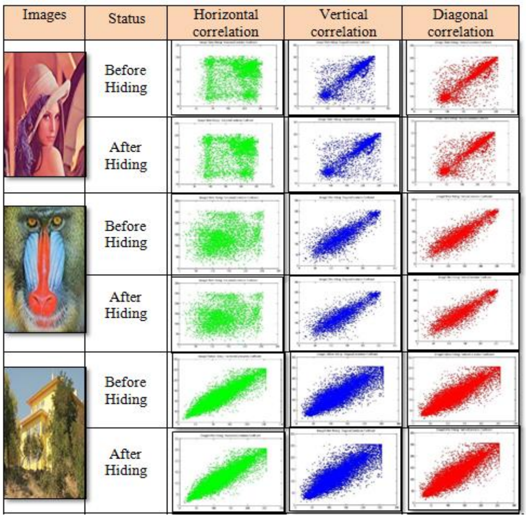


Fig. 8: The Correlation Test.

Fig. (9, 10 and 11) illustrate the histogram for the images before and after embedding the secret message (encrypted voter's information) in three color bands (Red, Green and Blue).

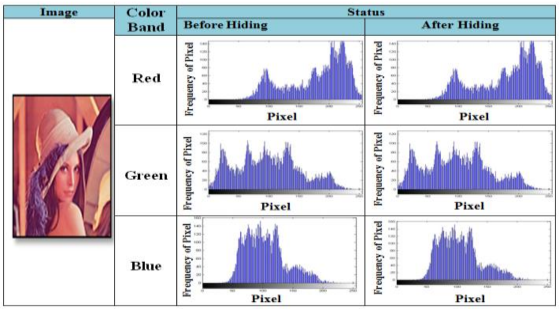


Fig. 9: Histogram Test for Lena Image.

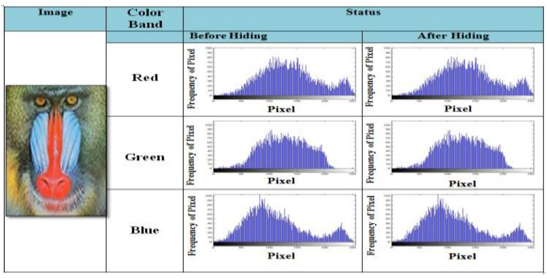


Fig.10: Histogram Test for Manderil Image.

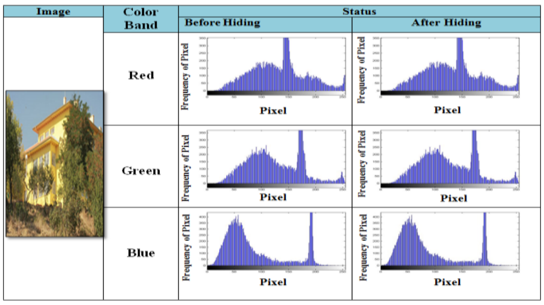


Fig. 11: Histogram Test for House Image.

Conclusions

The design and implementation of the proposed system satisfies the following:

1) The proposed system greatly reduces the risks, as the hackers have to find the voter fingerprint image, PIN, PSO initial values, secret keys of ECC and the logistic maps parameters to be able to change the election results. This makes the election procedure to be secure against a variety of fraudulent behaviors.
2) The simulation results show that the PSO algorithm provided a high optimization and accuracy in extraction of a unique feature from the fingerprints image because the selected locations by PSO are concentrated around the center of the fingerprint image.
3) The algorithm chooses random integer K for each point and each number in the plaintext is encrypted in to two different points, so that the ECC algorithm is much difficult to decrypt by any attacker. In spite of the ECC is a more powerful and secure encryption algorithm, it needs more implementation time than other encryption algorithm.
4) The proposed hiding method (Multiple Chaotic Logistic Maps) added more level of security to the system because it is very sensitive to its initial condition and control parameter, so that any change in these parameters will prevent reaching the same hiding locations. As a result the hackers will not be able to extract the hiding information. The least significant bit (LSB) keeps the cover image with least distortion after embedding the voter information to it.

References

J.B.Humphreys,(1961), Effect of composition on the liquidus and eutectic temperature and on the eutectic point of cast irons, *BCRIAJ*,19,609-621.

S. Katiyar, K. R. Meka, F. A. Barbhuiya and S. Nandi, (2011), Online voting system powered by biometric security using steganography, *Second International Conference on Emerging Applications of Information Technology (EAIT), IEEE*, pp: 288-291.

L. Rura, I. Biju and H. K. Manas, (2011), Secure Electronic Voting System Based on Image Steganography, *IEEE Conference on Open Systems (ICOS2011)*, pp: 80-85.

A. K. Vishwakarma and A. Kumar, (2011), A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme, *International Journal of Technology and Engineering System (IJTES)*, Vol.2, Issue 1, pp: 8-11.

M. Vijay, S. Suvarna, K. Dipalee, and S. K. Patil, (2013) ,Face Base Online Voting System Using Steganography, *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3, Issue 10, pp: 462-466.

B. B. Kharmate, S. S. Shaikh, P. R. Kangane and T. Anant, (2015), A Survey on Smart E-Voting System Based On Fingerprint Recognition, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, Issue 9, pp: 8093-8100.

M. M. Jazzar, (2010), Feature Selection Based Verification System Using Fingerprint and Palm Print, PhD Thesis.

S.Talukder, (2011), Mathematical modelling and applications of particle swarm optimization, *Blekinge Institute of Technology*, PhD Thesis.

Q. Bai, (2010), Analysis of Particle Swarm Optimization Algorithm*, Computer and Information Science*, Vol. 3, Issue 1, pp: 180–184.

R. L. Rivest, A. Shamir, and L. Adleman, (1978), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, Vol. 21, Issue 2, pp: 120-126.

R. Afreen and S.C. Mehrotra, (2011), A Review on Elliptic Curve Cryptography for Embedded Systems, International Journal of Computer Science & Information Technology, ISSN: 09754660**,** *Academy & Industry Research Collaboration Center (AIRCC)* **,**VOL.3 ,pp. 84-103.

M. Brown, D. Hankerson, J. Lopez and A. Menezes, (2009),Software Implementation of the NIST Elliptic Curves Over Prime Fields, *citeseer*, , Available at http:// citeseer.ist.psu.edu/brown01software.html.

A. M. B. Witwit, (2001), Audio in audio steganography using wavelet transformation***,*** *M.Sc. Thesis*.

A. A. Shejul, U. L. Kulkarni, (2011), A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform, *International Journal of Computer Theory and Engineering*, Vol.3, Issue 1, pp: 16-22.

V. K. Sharma, V. Shrivastava, (2012), A Steganography Algorithm for Hiding Image in Image by Improved Lsb Substitution By Minimize Detection, *Journal of Theoretical and Applied Information Technology*, Vol. 36, Issue 1, pp: 1-8.

P. Amit, Z. Goseph, (2011), A Chaotic Encryption Scheme for Real-time Embedded Systems: Design and Implementation, *Department of Electrical and Computer Engineering, Iowa State University, Ames, USA*.

Maqableh, Mahmoud, Mohammad,(2012) ,Analysis and design security primitives based on chaotic systems for ecommerce, *PhD Thesis*. Durham University.