Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (23), August (2019)

ISSN: **2616-9185**

www.mecsj.com

Face Recognition Integrated with Chaotic Encryption for Secure Electronic Election Application

Zinah Jaffar Mohammed Ameen

Faculty of Computer Engineering

University of Technology, Baghdad, Iraq

Email: 120097@uotechnology.edu.iq

Abstract

Election is substantial right for every nation. An Electronic Election (E-E) system is an election system in which the voting process is performed, stored and handled digitally, that makes the election arrangement labor better than conventional paper based method. However, security remains a point of hardship for each system. Therefore, the necessity of designing a secure E-E system is very important. This paper introduced a secure e-e web application. Depending on secure authentication process based on face recognition besides encrypting the single elector's choice.. A Local Neighborhood Intensity Pattern (LNIP) of feature descriptor method is imposed to distinguish the permitted and authorized electors. An effective framework using a modified 3-3-2 LSB method to conceal the electors' choice within his own instant image captured for recognition process, then a chaotic encryption based on a three-dimensional Lorenz map is proposed to encrypt the stegano image before forwarding to the server.

Keywords: Web application, LNIP recognition face, LSB steganography and Lorenz map.

1. Introduction

Many proposals for election systems have been made since 18th century. Several studies to improve the process of election using electronic technologies. When designing an e-election system, it is important to consider ways in which the election tasks are performed electronically without revealing electors' privacy or leading to opportunities for malpractice [1]. Integrity of the election process is an important matter in the honesty of the democracy itself. Therefore, the whole arrangement of election must guarantee security and robustness against a variety of deceitful behaviors [2]. There is no quantification for agreeable security norm, because the norm relies on type of the information. An agreeable security level is always a compromising between usability and strength of the security method [3]. In the recent years, automated method of distinguishing a person is going to be more widespread by using biometric system. A biometric has shown growing concern in many fields such as surveillances, computer interfaced with human and security identification. Biometric discrimination is an automated method of distinguishing an individual by means of matching the feature vector extracted from the behavioral and the physiological distinctiveness such as finger print, iris, face recognition etc. [4]. Face recognition and distinguishing is becoming progressively important. There are multiple references available and can be used as features. Facial features are derived and compared using pillar vector machine classification algorithm [5]. This paper is organized as follow section 2 discusses the previous related work, section 3 summarizes the secure e-election system, section 4 explains the proposed system design and implementation. Finally conclusion is discussed in section 5.

2. Related work

Firas Hazzaa et al [1] proposed an e-election system relied on fingerprint performed using C#. Neha Gandhi [2] introduced an online election system relied on fingerprint then, the result was encrypted using SHA 256 with MD5. Patil R. H. et al [6] proposed a secure e-election system based on face recognition and dactyl gram technique. A. Geetha et al [7] performed a face detection algorithm depent on local derivate tetra pattern. Jain et al [8] proposed an adaptive circular queue image steganography with RSA cryptosystem. Ye et al [9] suggest an influential framework for chaotic encryption based on a three-dimensional logistic map together with secure hash algorithm-3 (SHA-3) and electrocardiograph (ECG) signal. Li et al [10] examined the security properties of the image encryption algorithm based on information entropy (IEAIE) and rated the validation of the used quantifiable security features.

3. Secure E-Election System

E-election application is a public election system based on web exploited to make election process easier to use and quicker [6]. The aim behind the development of such system is to facilitate the process of arranging elections and make it easy for electors to elect remotely from their pcs or smart devices taking into account better security, secretion and providing auditioning abilities [3]. Problems such as forbidden unauthorized election, improper use of cryptography, susceptibility to network threatening. E-election system is more vulnerable to attacks such that election results can be tampered simply hence may result in fraudulence. To revoke those problems this paper suggested the use of face recognition in order to verify the eligible electors' identity, then electors' choices would be encrypted twice first using with steganography technique, then cryptography methodology.

3.1 Facial Recognition

Biometrics is becoming a major element of a subjective identification solution, since biometric identifiers cannot be shared or mislaid, and they represent any personal's identity. Biometric identification references to the use of iris, fingerprint, face palm and speech distinctive called biometric identifiers [1]. In previous years, face recognition plays an important role in many powerful researches. With the current world security status, governments as well as private sector demand dependable methods to recognize individuals precisely without contradicted with rights or privacy. 'Many mechanisms have been utilized to face estimation and they can be subdivided into two categories [7]:

- Geometric feature matching.
- Template matching.'

The efficiency of face recognition mechanisms have severely increased. However, the strength of face recognition technique needs improvement. The consequences of such techniques affected by 'environmental changes, such as illumination deviations, expression disparity and pose variations '[11].

Local Binary Pattern (LBP) is a grayscale invariant texture calculation, it is a beneficial tool to design texture images. LBP has shown a magnificent efficiency in many comparative studies, in terms of both velocity and differentiation performance. In this tool, a small window of an image is taken first, then the intensity difference between the center pixel and its N neighbors are measured [12].

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (23), August (2019)

ISSN: **2616-9185**

www.mecsj.com

The primary LBP operator labels the pixels of an image by considering the threshold value of the 3 × 3 neighborhood of each pixel with the central pixel value concatenated the results to form a number. As clarified in figure (1), locating an LBP micro pattern when the threshold reaches zero [11].

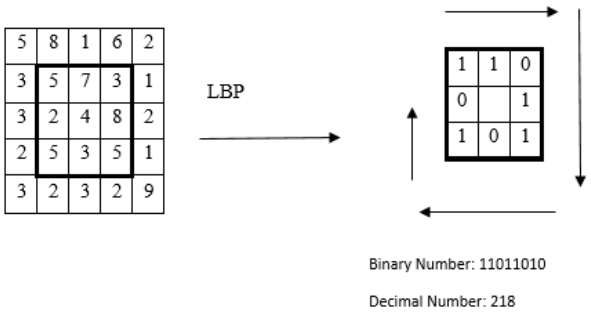


Figure (1) LBP Operator

LBP local pattern is found by differentiating between the centered symmetric pixels and neighboring pixels without taking into account the other relative intensity difference between each pixel and other adjoining pixels other than the center one. Therefore, an updated LBP algorithm, Local Neighborhood Intensity Pattern (LNIP) is chosen in this paper, LNIP observes two neighboring pixels for binary pattern computation and the radius of unit distance. As the nearest neighboring pixels carries more distinctive information for texture descriptors. Thus by using a 3×3 window for computing the binary pattern by examining the mutual information with respect to the adjacent neighbors. Figure (2) explains the adjacent neighbors in a 3×3 window.

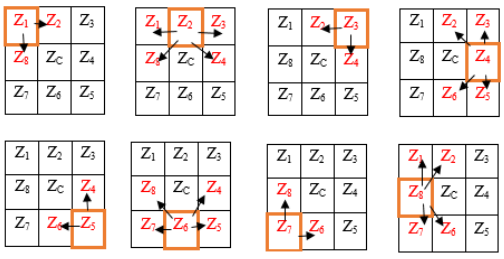


Figure (2) the adjacent neighbor relation

As shown above the neighboring relations for each of the 8 adjoining pixels of Z_C, Z_i has 4 adjoining pixels if (i) is even otherwise, Z_i has only 2 adjoining pixels for odd values of i.

For signed $LNIP_S$, the sign of proportional variation between one of the 8 neighboring pixels according to the center pixel (Z_C) and its corresponding adjoining neighboring Z_i. An N little pattern with respect to Z_i where N is the number of element in S_i. A binary pattern $A_{1,i}$ corresponding to Z_i using equation (1). Similarly, another binary pattern $A_{2,i}$ of same size taking into consideration the same neighboring as in S_i using equation (2).

$$A_{1,i}(j) = \text{Sign}(S_i(j), Z_i) \text{ where } j = 1 \text{ to } N \quad \text{Eq. (1)}$$

$$A_{2,i}(j) = \text{Sign}(S_i(j), Z_C) \text{ where } j = 1 \text{ to } N \quad \text{Eq. (2)}$$

The single bit according to Z_i it is simply evaluated by measuring change in the construction of these two are binary patterns $A_{1,i}$ and $A_{2,i}$. The structural change in the bit pattern is computed by taking bitwise XOR operation between these two patterns. In order to calculate the information of total deviation of these neighbors from a particular pixel (Z_i) $LNIP_M$ is used.

$$M_i = \frac{1}{M}\sum_{j=1}^{M} | S_i(k) - Z_i | \quad \text{Eq. (3)}$$

$$T_C = \frac{1}{8}\sum_{i=1}^{8} |Z_i - Z_C| \quad \text{Eq. (4)}$$

M_i is the mean deviation about the i^{th} neighboring of Z_c from its corresponding S_i as indicated in equation (3) calculated for all the 8 neighboring pixels of Z_c in a 3 × 3 window. T_c is the threshold value examined by taking the mean deviation of the neighboring Z_i about the center Z_c as shown in equation (4). The final magnitude pattern value corresponding to Z_c is evaluated using equation (5).

$$LNIP_M(Z_c) = \sum_{i=1}^{8} 2^{i-1} \times Sign(Z_i, T_c) \quad \text{Eq. (5)}$$

These additional steps were mandatory to make the patterns immune to illumination changes and the mutual relationship among the adjoining neighbors is well explored in this pattern. Besides that, not only the sign of the intensity difference between the central pixel and one of its neighboring pixels Z_i was taken into account, but also the sign of difference values between Z_i and its adjacent neighbors along with the central pixels. Most of the local patterns including original LBP concentrates mainly on the sign information neglecting the magnitude. The sign information is more substantial for any binary pattern, it cannot be eliminated as it plays an auxiliary part to supply complementary information texture descriptor. Therefore, both sign pattern $LNIP_S$ and magnitude pattern $LNIP_M$ poses complementary information that gives superior performance as compared with the original LBP [12].

3.2 Chaos and Chaotic System

Chaos theory a mathematical physics, was evolved by Edward Lorenz and it is a sureness and randomly determined stochastic process appearing in a nonlinear dynamic system. Even the theoretical studies on the behavior of systems shows that many of them follow deterministic laws, but on the other side they look random and unpredictable and have a sensitive dependence on their initial conditions; small changes in those conditions can lead to quite different outcomes [13].

Chaotic systems have a number of curiosity properties besides sauvity to premier situation and system parameter, periodicity and confusion (expansion and folding) properties, etc. These properties make the chaotic systems an attractive choice for establishing the cryptosystems besides their sensitivity to the premier situation/system parameter and confusion properties are similar to the mixing and spread processes of a good cryptosystem. In ideal cryptosystem confusion process decreases the correlation between the propagation and image encryption while diffusion process turn the pixel value of the coordinate. In other words, the confusion stage changes the position of data while the data itself is changed during the diffusion process [14].

There are two kinds of image encryption position permutation and value transformation. In position alternation mechnism, altering the image position without changing pixel's value of the original image, but in value transformation technique pixel's value is replaced by another pixel's value without changing position. XOR operation is one of the most used value transformation technique, used to create linear independency between two or more arguments. The idea behind using XOR encryption its difficult to be reversed without knowing the initial value of one of the two arguments. In order to improve the security performance of the image encryption algorithm, the concept of shuffling the positions of pixels in the plain-image and then altering the gray values of the shuffled image pixels is used [15]. Chaotic maps are used in many proposed encryption methods. These maps are sensitive to initial condition, unpredictability and mixing properties. Because of these features, they can guarantee more secure encryption methods [16]. At this stage, usually reversible operations such as XOR, AND are used [17]. This paper proposes using a three-dimensional Lorenz chaotic map. The Lorenz system of differential equations is one of the most famous models of nonlinear dynamic system which exhibits a chaotic properties for certain initial values and system parameters are described by equation (6):

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= bx - xz - y, \\ \dot{z} &= xy - cz, \end{aligned} \qquad \text{Eq. (6)}$$

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (23), August (2019)

ISSN: **2616-9185**

www.mecsj.com

The superscript dots denote a time derivative argument (ẋ = $dx/$, $etc.$). Three variables (x, y and z) are required according to (Poincare-Bendixson theorem), which states that chaotic behavior can only occur in continuous dynamical systems whose phase space has three or more dimensions. This theorem is not applicable to discrete dynamical systems, where chaotic behavior occurs in two or even one-dimensional system. There are three parameters, which Lorenz took σ = 10, r = 28, and b = 8/3, are no chance.

Linearly re-scaling the variables x, y, z and t is possible, so that four of the seven terms on the right hand side of equation (6) have coefficients of 1.0. The choice of deciding the position of the remaining coefficients is arbitrary, but Lorenz chose to represent them as the Prandtl number (σ), the Rayleigh number (r), and the Aspect ratio of the convection cylinders (b) [18].

Figure (3) shows the chaos 3D Lorenz map phenomena depends on the given initial conditions and starting at (100, 0, 200), hence it produces three different chaotic sequences.

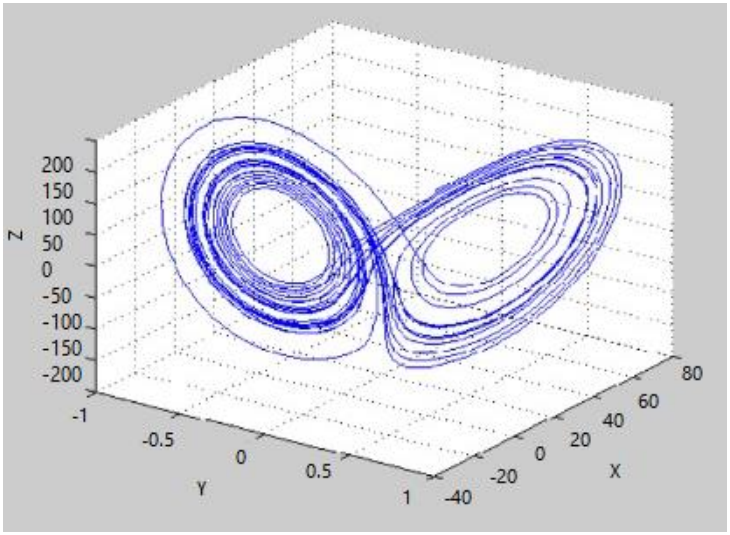


Figure (3) 3D Lorenz Map

Presence of cubic coupling with three parameters make the 3D Lorenz map more secure. Figure (4), (5) and (6) indicate the time and frequency representation of X, Y and Z components.

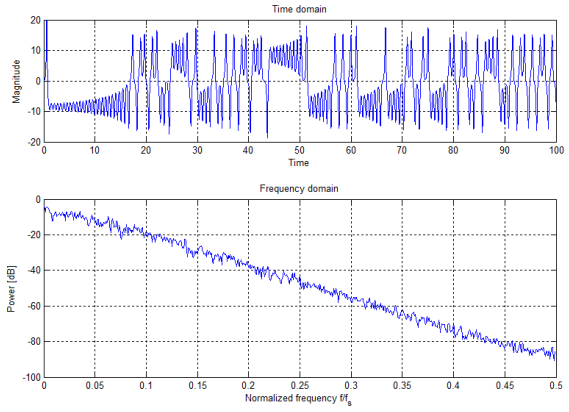


Figure (4) X Component Plot

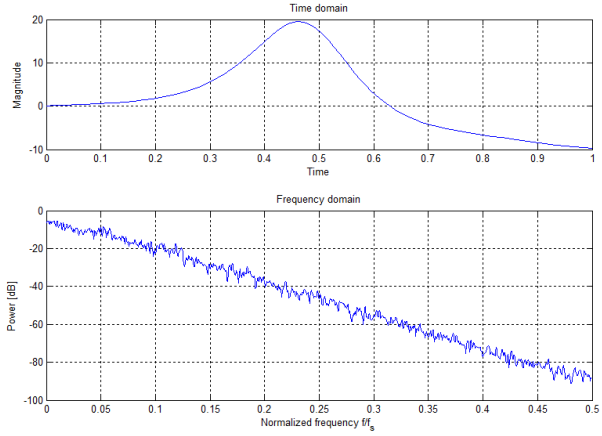


Figure (5) Y Component Plot

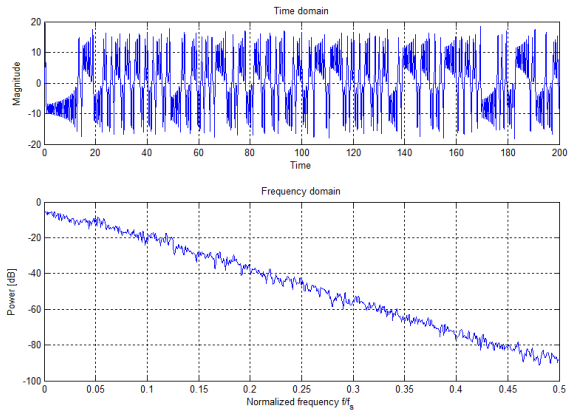


Figure (6) Z Component Plot

3.3 Steganography

During recent trends of technology, the challenge of improving Information security became an important need, especially when sending and receiving data through the Internet. Many techniques were used to protect the users' sensitive data from unauthorized access during transmission. Cryptography, watermarking and steganography are the common methods used to secure digital data, but the most efficient techniques are cryptography and steganography applied in Information Hiding [19]. Watermarking method embeds specific information within digital data to prevent unauthorized tampering [16].

Cryptography has many encryption algorithms used to convert the transferred data into unrecognizable form keeping it away from unauthorized access.

Many advanced mathematical procedures are included within encryption and decryption algorithms to make them more complex and hence increasing the security level [19].

Steganography method is used to embed information within a cover image randomly. It provides a simple and strong way to conceal secret information within selected image as a cover. Thus, reducing the chance of the cover image being detected, such that the secret message is concealed in such a way that preserves the quality of the covered image. Based on chaotic chart and human visual characteristics a large capacity of stenographic techniques are proposed. Experimental results show substantial enhancement in capacity and invisibility, such as robustness to image processing techniques like image cropping compression, etc. [13]. The Lorenz map is used to generate a sequence as the watermark, which is used to shuffle the bits order of the secret message.

Generally, there are two known methods for steganography. Transform domain and spatial domain. Transform domain methods used conversions for embedding secure message in cover media. The transforms are included: DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform). In spatial domain method, the secret message is concealed directly within the cover media [16]. The image in which a confidential message would be concealed is called the stego-image. There are different categories of spatial domain, (i) LSB steganography, (ii) RGB based steganography, (iii) pixel value differencing steganography, (iv) mapping based steganography, (v) palette based steganography, (vi) collage based steganography, (vii) spread spectrum steganography, (viii) code based steganography, and (ix) others. Least Significant Bit (LSB) is one of the most well-known algorithms in spatial domain [16]. In the base mechanism eight-bits technique of confidential data are behold for inclusion at a time in the LSB of RGB pixel value of the carrier image in 3, 3, 2 order respectively.

Thus first three bits of the secret message are concealed inside three (03) bits of LSB of Red pixel, next three bits in the three (03) bits of LSB of Green pixel. The remaining two bits of secret message are concealed in two (02) bits of LSB of Blue pixel [13].

To improve the 3-3-2 LSB approach, two different techniques is applied. The first technique is known as 2-1-1 LSB technique and second is known as 1-2-1 LSB technique. They both are used in combination to hide the complete message as shown in Figure (7) for one pixel.

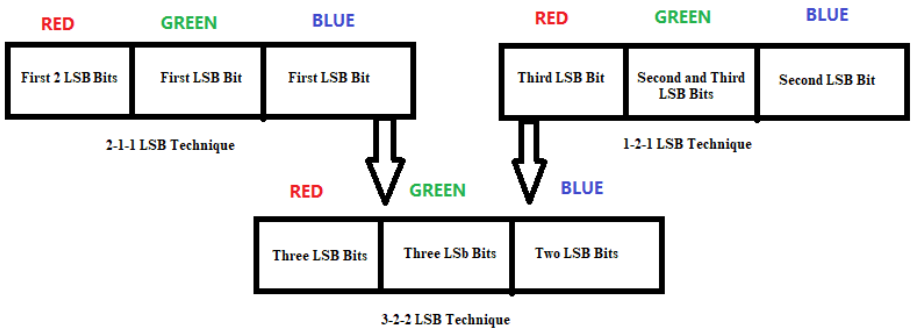


Figure (7) Enhanced 3-2-2 LSB Approach for one Pixel

The major processes of the stegosystem based on enhanced 3-2-2 LSB encoder are sketched in figure (8).

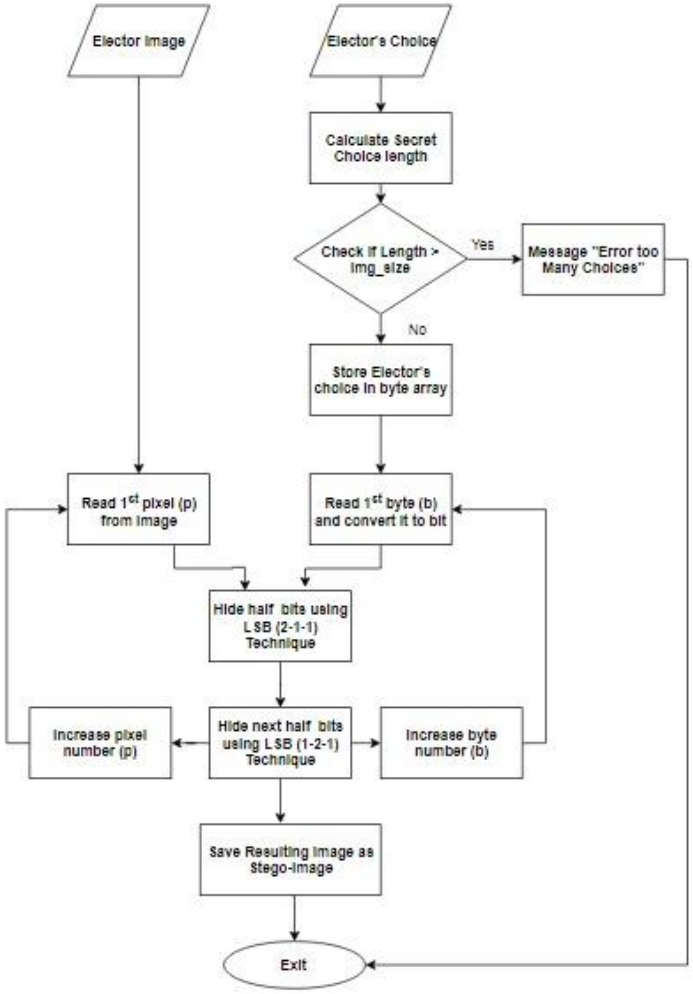


Figure (8) Stegosystem using LSB 3-2-2 modified Technique

4. Proposed System Methodology

This section discusses design and implementation of proposed secure electronic election web application.

A. System Design

Figure (9) summarizes the use case diagram for the administrator and single electors who deal with this system. The main tasks for both of them is shown in this figure, the administrator is responsible for managing the whole electing process specially registering people who are allowed to vote that is forbidden to be done by individual electors. On the other hand, electors have only to enter their voter's ID number as written in their electoral card besides capturing an instant image for authorization process.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (23), August (2019)

ISSN: **2616-9185**

www.mecsj.com

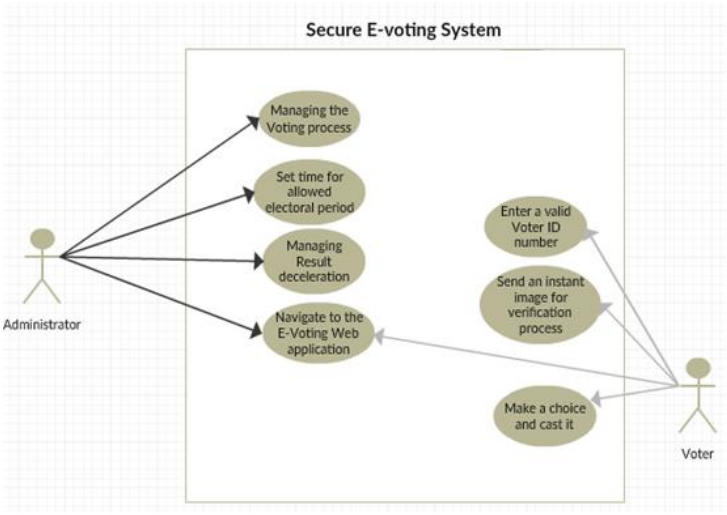


Figure (9) System Use Case Diagram

The authorization process applied in this system is relied on face recognition. Face recognition procedure summarize in figure (10). Image retrieval from server is implemented using LNIP feature descriptor of stored images, based on previous equations to retrieve images with highest matching values and put them at the beginning in order to decide whether this person could vote or not.

To enhance the effectiveness of transmission and keep safety from attacks by intruders, so the proposed method can achieve higher level of data integrity, confidentiality and security especially remotely voting, this secure e-voting system provides besides secure login, additional security issues represented by steganography and Chaotic ciphering. Figure (11) presents the ciphering method implemented in this system for safely casting voter's choice. By using the enhanced 3-2-2 LSB approach in order to conceal the elector's secret choice with his/her the input image, with resolution of 256×256 pixels as a cover image.

The architecture of the proposed encryption is represented in figure (11), for a given input image after converting it to gray each pixel is represented by an 8 bit binary sequence for 256 gray scale. To achieve an effective bit level permutation, the confused image would exclude any repeated patterns. Then the diffusion phase has an important role in encryption, based on bit level permutation the position of each pixel would be exchanged and pixels' values are modified. The output ciphered image is posted to the server.

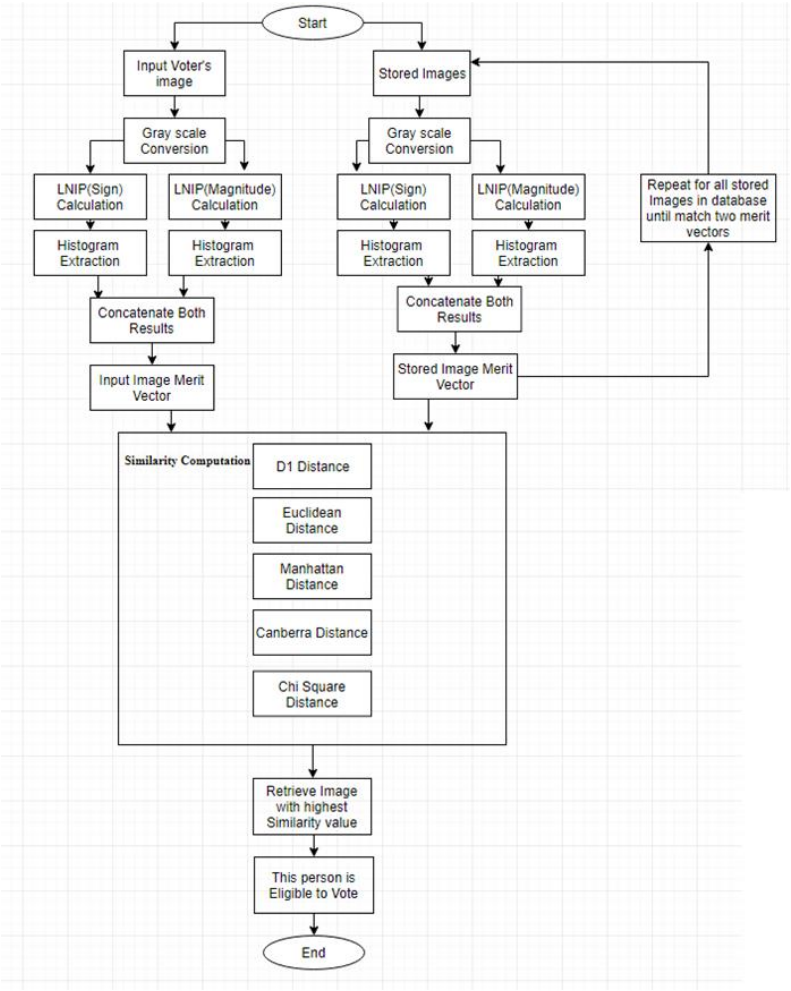


Figure (10) Flow Diagram of Face Detection Methodology

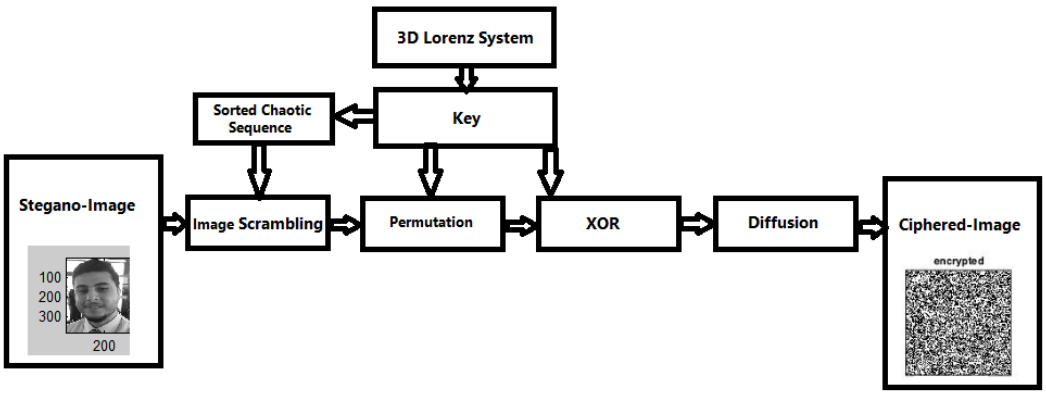


Figure (11) 3D Lorenz Encryption

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (23), August (2019)

ISSN: **2616-9185**

www.mecsj.com

B. System Implementation

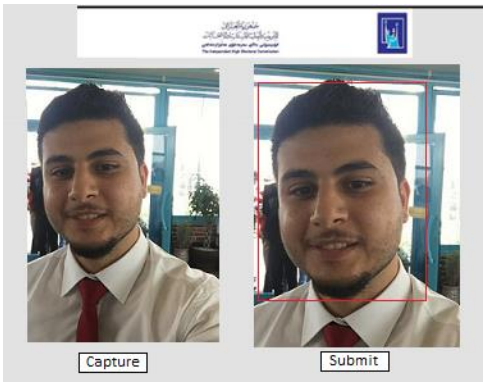
For implementing this system PHP version 5.6 is used with SQL server version 5.2 for implementing server side scripting side by side with Matlab version 9.1 to implement image processing algorithm then hide the elector's choice using modified 3-2-2 LSB approach and finally encrypt the stegano-image with chaotic 3D Lorenz map.

Figure (12) Administrator Login

First the administrator should login to activate the system as indicated in figure (12).As the electoral period is started, electors are able to access the application and vote as shown in figure (13). The eligible electors require an ID number besides an instant image to verify their identity. An instant image is capturing with limited size of 512×512 with clear Facial features as shown in figure (14).

Figure (13) Voter Login

(A)



(B)

Figure (14) Elector's instant image

In case if the entered ID number is correct and elector's image retrieved from server database, a elector ID card information would be presented as indicated in figure (15).

Figure (15) Elector ID card Information

Each eligible elector is allowed to vote only once, otherwise a message indicating that the person with this ID number had already been voted and is unable to vote again as shown in figure (16).

Figure (16) Election right is done only once

A good encryption should be resistance to any kinds of attacks, such as differential attack, known lain text attack and etc. this system were simulated on 512×512 of ten elector, each one with 4 images stored in the database. The achieved recognition rate was 75%, with total average computation time 21.305 s. for image encryption and decryption per user login. Figure (17) shows the experimental results for encrypted and decrypted image.

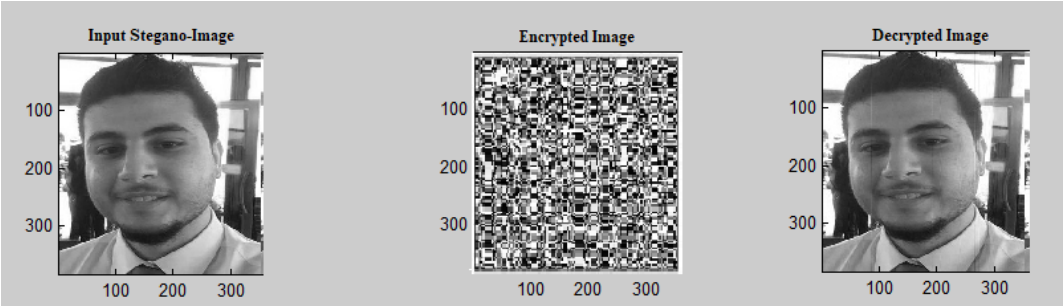


Figure (17) Original (Stegano-image) and cipher image

The histogram of the image before and after encryption is shown in figure (18), are compared to analyze the statistical performance. The histogram of the cipher image can give information of the original image if it is not uniform enough, a mass information may be analyzed by an intruder.

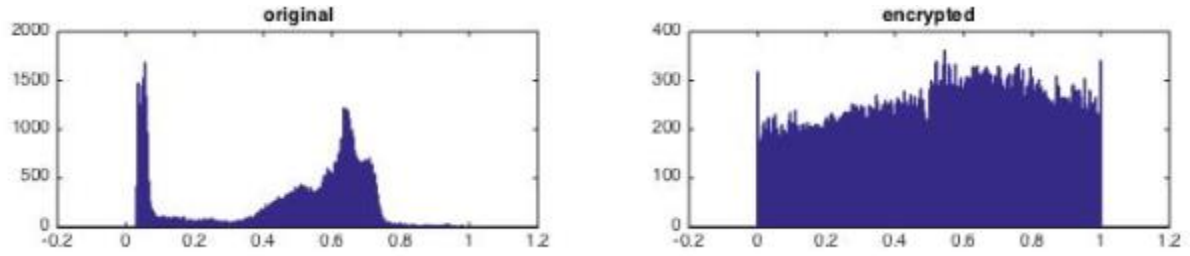


Figure (18) The histogram of Original and Encrypted Images

5. Conclusion

This paper discusses the designing and implementing of a secure E-Election web application. Security is provided in two approaches, first one the elector's authorization process is performed based on (LNIP) approach for face recognition besides his/her unique voter ID number, otherwise he/she would be deprived the election. Second approach and to ensure that each elector's choice is transferred as it is securely without altering, Cryptography and steganography methodologies are used to introduce two levels of security. The modified 3-2-2 LSB approach is applied, in which the secret message is converted to some other form at first before hiding within the cover image in order to enhance its security level. This approach is used to encrypt an elector's choice to provide confidently at the first level using his/her instant image as a cover to form a stego-image, then the output image is encrypted using 3D Lorenz chaotic map and the encrypted image will be posted to the server. If any attack by a hacker or eavesdropping is happened, it would be difficult to him to retrieve the original text especially within the allowed electoral period. This system was tested on ten persons; six were recognized and able to vote. The achieved recognition rate was 75%, with total average computation time 21.305 s. for image encryption and decryption per user login. This system validates that secure E-Election application is feasible and satisfactory.

References

[1] Firas Hazzaa and Seifedine Kadry, “New System of E-Voting using Fingerprint”, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, October 2012.

[2] Neha Gandhi, “Study on Security of Online Voting System using Biometrics and Steganography”, International Journal of Computer Science and Communication, Volume 5 No.1, September 2014.

[3] Alaguvel. R, Gananavel. G and Jagadhambal. K, “Biometrics using Electronic Voting System with Embedded Security”, International Journal of Advanced Research in Computer Engineering and Technology”, Volume 2, Issue 3, March 2013.

[4] Mukesh D. Rinwa and Bharat S. Borkar, “Face Recognition using Local Patterns”, International Journal on Recent and Innovation Trends in Computing and Communication”, Volume 3, Issue 10, October 2015.

[5] M.N. Annadate, Shreyans Sunil Gandhi, Nivita Ravi Kaniampal and Pushkar Satish Naral,”Online Voting System using Biometric Verification”, International Journal of Advanced Research in Computer and Communication Engineering, Volume 6, Issue 4, April 2017.

[6] Patil Rahul H., Tarte Babita B., Wadekar Sapana S. and Zurunge Bahakti S., "A Secure E-Voting System using Face Recognition and Dactylogram", International Engineering Research Journal, Volume 2, Issue 2, 2016.

[7] A. Geetha, M. Mohamed Sathik and Y. Jacob Vetharaj, "Face Recognition based on Local Deivative Tera Pattern", Journal on Image and Video Processing, Volume 7, Issue 3, February 2017.

[8] Mamta Jain, Saroj Kumar Lenke and Sunil Kumar Vasistha, "Adaptive Circular queue image Steganography with RSA cryptosystem", Perspectives in Science, Elsevier, Volume 8, September 2016.

[9] Guodong Ye , Kaixin Jiao, Chen Pan, and Xiaoling Huang, "An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map", Security and Communication Networks, Hindawi, https://doi.org/10.1155/2018/8402578, 2018.

[10] Chengqing Li, Dongdong Lin, Bingbing Feng, Jinhu Lü and Feng Hao, "Cryptanalysis of a Chaotic Image

Encryption Algorithm Based on Information Entropy", IEEE Access, Vol. x 4, Digital Object Identifier 10.1109/ACCESS.2018.DOI, 2018.

[11] Sharadamani and C. Naga Raju, "Face Recognition using Gradient Derivative Local Binary Pattern", International Journal of Applied Engineering Research, Volume 12, No. 7, 2017.

[12] Baochang Zhang, Yongsheng Gao, Sanqiang Zhao and Jianzhuang Liu," Local Derivative Pattern versus Local Binary Pattern: Face Recognition with High-Order Local Pattern Descriptor", IEEE Transactions on Image Processing, Volume 19, No. 2, February 2010.

[13] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Manda and Paramartha Dutta, "A Novel Secure Image Steganography Method Based On Chaos Theory in Spatial Domain", International Journal of Security, Privacy and Trust Management, Vol 3, No 1, February 2014.

[14] Sandhya Rani M.H. and K.L. Sudha, "Design and Implementation of Image Encryption Algorithm Using Chaos", International Journal of Advanced Computer Research, Volume-4 Number-2 Issue-15 June-2014.

[15] Md.Billal Hossain, Md.Toufikur Rahman, A B M Saadmaan Rahman and Sayeed Islam, "A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component", 3rd International Conference on Informatics, Electronics & Vision, IEEE, 2014.

[16] Milad Yousefi Valandar, Peyman Ayubi and Milad Jafari Barani, "High Secure Image Steganography Based on 3D Chaotic Map", International Conference on Information and Knowledge Technology, IEEE, 2015.

[17] Ahmad Shokouh Saljoughi and Hamid Mirvaziri, "A new method for image encryption by 3D chaotic map", Pattern Analysis and Applications, Springer, https://doi.org/10.1007/s10044-018-0765-5, 2018.

[18] Md. Shakhawat Alam and Payer Ahmed, "Several Chaotic Analysis of Lorenz System", European Scientific Journal, Vol.13, No.9, March 2017.

[19] May H.Abood, "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms", Annual Conference on New Trends in Information & Communications Technology Applications, IEEE, 2017.