

A NOVEL GROUP-BASED CRYPTOSYSTEM BASED ON ELECTROMAGNETIC ROTOR MACHINE

ASHISH KUMAR^{a1} AND N S RAGHAVA^b

^{ab} Delhi Technological University, Delhi

ABSTRACT

In this paper, an algorithm is aimed to make a cryptosystem for gray level images based on voice features, secret sharing scheme and electromagnetic rotor machine. Here, Shamir's secret sharing (k, n) threshold scheme is used to secure a key along with voice features of $(n - k)$ users. Keystream is molded by coefficients of a voice sample, using this key stream, rotor machine's rotating cylinders' positions are initialized and internal wiring is decided by pseudo random number of Hénon chaotic map, where initial seed for chaotic system is chosen from keystream. And furthermore, shares of key stream are distributed among users. Speech processing is fused with electromagnetic machine to provide authentication as well as group based encryption. Perceptual linear predication (PLP) coefficients are utilized for formation of secret key. Simulation experiments and statistical analysis demonstrate that the proposed algorithm is sensitive to initial secret keystream, entropy, mean value analysis and histogram of the encrypted image is admirable. Hence, the proposed scheme is resistible to any vulnerable situation.

Keywords: Electromagnetic machine, Hénon chaotic map, PLP coefficient, secret sharing scheme

With the recent growth of multimedia, Web world is now being focused upon multimedia-based information over internet; due to this security is an important key concern while transmitting or storing information [1]. There are two types of cryptography method which is used to secure information. One of them is symmetric key cryptography [2], [3] and another one is asymmetric key cryptography. In asymmetric key cryptography scheme both sender and receiver use the different key. In traditional cryptography system, it was difficult to secure large size of multimedia from intruder or attackers and calculation of mathematical equation (built-in Encryption technique) was not so easy therefore many researchers worked upon the security of bulky information. In this series, Chaotic system, biometric features, confusion and diffusion are materialized in cryptography followed the concepts of tradition cryptography. Rotor cipher was effectively used in past; Enigma machine is an example of Rotor Machine. The Enigma machines were developed as a chain of electro-mechanical rotor cipher machines and used in the Era of mid-twentieth century to protect confidential information, diplomatic and military communication. Arthur Scherbius Enigma invented enigma machine at the end of World War II [4]- [5]. Enigma machine has a set of independent wheels through which the electric pulse can flow to other wheels. Each cylinder or wheel has fixed amount of input pins and output pins. Each input pin is connected to a unique output pin of the cylinder. So there is a unique path between input pins and output pins.

If machine has three cylinders or wheels, then it is categorized into fast rotor, medium rotor and slow rotor. Whenever any input is given, fast rotor is shifted circularly in clockwise

direction and according to prior connections of wires, internal connections between pins are also shifted towards the rotor movement. A rotor with n number of labels completes its one rotation after n number of inputs. When fast rotor completes one cycle then middle rotor rotates in clockwise direction by unit position. Slow rotor shifts one position to right after one complete cycle of middle rotor. This movement makes the system dynamic in nature.



Fig. (a) :War-damaged Enigma rotor A7135 (b) Three rotors on their shaft (c) Original Enigma "D" Reflector number A5221

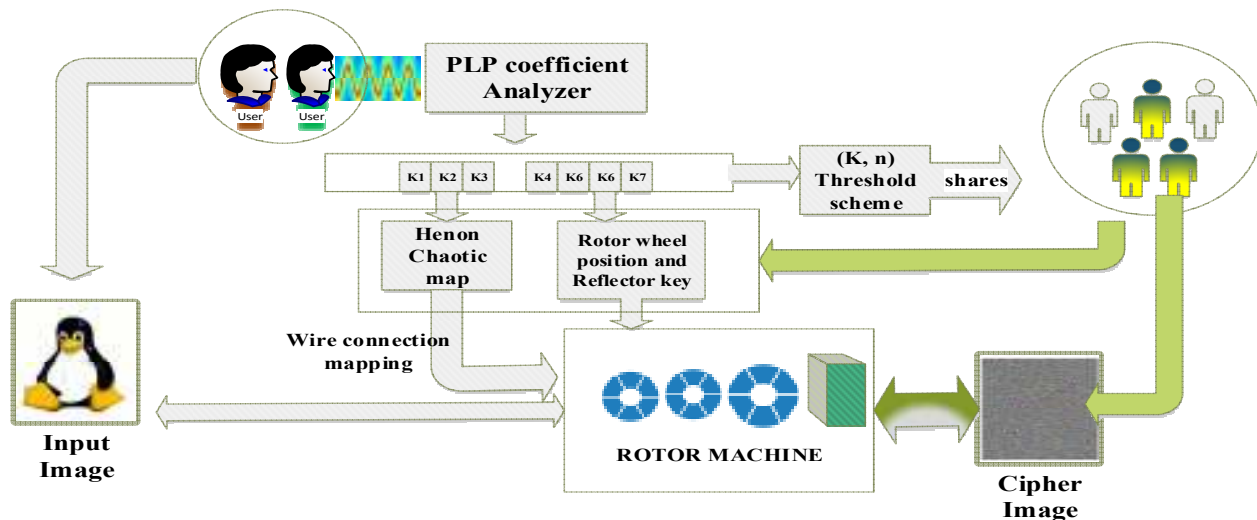


Fig.2: The architecture of Proposed Cryptosystem

Every person has their own way to speak a language, this voice sample is preprocessed and further synthesized for various applications such as authentication. When any person speaks, the sound is perceived by human ear or machine. MFCCs (Mel Frequency Cepstral Coefficients) and PLP (perceptual linear prediction) coefficients of Voice are unique biometric features which can be used to provide security services according to security requirements [8]- [9]. In PLP perceptual property of human ear is captured. Power spectrum of speech signal in bark scale is equivalent to human's perceptual model. MFCC coefficients are found under the Mel scale filters which are triangular filters whereas PLP coefficients are found under Bark scale filters which are trapezoidal in shape. In cryptography speech processing is being used with other biometrics at the vast level for reliable security systems.

Related Work

Zhi-liang ZHU et al. proposed an encryption method based on the nonlinear mechanism of the Enigma machine and chaos controlling the encryption process [10]. In paper [11], Elkamchouchi and Elshafee proposed a rotor-enhanced block cipher method to obtain permutation and substitution operations in which the rotor generates the round key to achieve cipher text key dependency. In paper [12], the author proposed a cryptographic system with an unbalanced rotor to achieve goals of permutation and substitution.

In [13], Chen et al. presented a symmetric image encryption scheme based on 3D chaotic cat maps. Wang et al. [14] introduced a 3D Cat map-based symmetric image encryption method which comes out to be computationally expensive and has a non-independent key space. Image encryption algorithms are constructed on the diffusion property of Shannon's theory where hyper-chaotic systems are

also presented in cryptosystems [15], [16]. In [21], Wahyudi, Astuti, and Syazilawati adopted PLP coefficients of voice to develop an intelligent voice-based door access control system.

PROPOSED METHOD

The proposed algorithm is designed with regard to sensitive information of digital images. The algorithm is performed within two groups where one group encrypts the input image with their voice segment and decomposes the secret key into shares and transmits them to another group. Therefore, in the first phase, key generation and encryption processes take place, where from group *A*, a person speaks from a sound acquisition device and this wave sample is converted into a keystream for the further process and after that designing the process of the rotor machine is done by the Hénon chaotic system. Here the cryptosystem is completely based on the concept of an electromagnetic rotor machine and the properties of the Hénon chaotic map. The rotor machine is a vital core part of the second phase of the algorithm.

Let us consider a digital color image I with dimension $M \times N \times 3$ (i.e. M rows and N columns). A digital color image is transformed into a gray scale image. This gray scale image supports $[0, 255]$ decimal values with 8-bit binary format of a computer system.

PLP (Perceptual Linear Prediction) Feature Through Voice Segment

Step 1: choose a speech acquisition tool to capture a voice segment and take 256 samples from this wave file.
Step 2: calculate FFT and calculate the power spectrum using the squared magnitude of the signal.

Step 3: convert frequency bin points to corresponding bark and bark scale is divided into equal 14 filters.

Step 4: calculate cube root of the power spectrum for each bark scale values.

Step 5: Bark scale is divided equally spaced triangular filters, width of filters equal to 5 bark scales with 50% overlap.

Step 6: Calculate IFFT of each triangular filter, these 14 values are known as PLP coefficients.

Step 7: out of 14 coefficients, 7 coefficients are chosen by the person to generate a keystream [17]- [18] and following steps which are given below:

$$\begin{aligned} \text{keystream} &\leftarrow K[7] \\ |K[7]| &\leftarrow K[7] \times 256 \\ K[7] &\leftarrow \text{MOD}(K[7], 256) \\ \text{Keystream} &\leftarrow K[7] \end{aligned}$$

Digital Electromagnetic Rotor Machine

Electromagnetic machines used in World War II to send secret information, where each rotor’s pins were labeled with 26 characters and mapping of wires within rotor was static all the time. So basically it was based on the initial position of the rotor and the wired mapping of reflector. Here we have designed a cryptosystem which is truly based on Electromagnetic machine concept. It is a digital model of electromagnetic machine to encrypt information with more number of combinations and dynamic wired mapping between pins, so it is hard to eavesdropper to deduce the original content from cipher. Here we have designed rotor with 256 input pins and each pin is connected with their corresponding output pins. Output pins label are generated using Hénon chaotic map and according to that, input pins are connected to output pins with their corresponding number. For example, a rotor has 4 pins. Initial rotor position starts from $K1 = 4$ and $K4$ be some number as initial seeds for Hénon chaotic map which generates a sequence, say, [3 2 1 4].

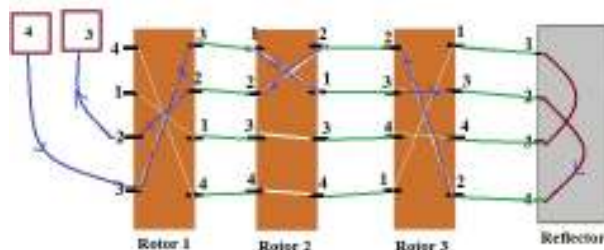


Fig.3: Wire connections within Rotor

Figure 3 illustrates the wiring connections among rotors and reflector. For the given example initial input at 4th pin gives output at 3rd pin. Output pins label of rotor 1 are generated using Hénon chaotic map and according to that, input pins are connected to output pins with their corresponding number. Blue path shows the flow of current within the model with respect to the input.

A.Algorithm for Encryption

Step 1: $K1, K2, K3$ are the initial seeds for Hénon chaotic map using (1), which generates the sequence for Rotor1 Rotor2 and Rotor3 respectively, as shown in fig. 2.

Step 2: keystream $K4, K5, K6$ are used to initialise the positions of all rotors in the machine. $K7$ is used to connect pins within reflector.

Step 3: Hénon chaotic map [19] discovered in 1978 is used as a pseudo random number generator in security systems. Two dimensional discrete-time nonlinear dynamical Hénon chaotic map generates pseudo-random binary sequence which has been described as below:

$$\begin{aligned} X_{n+1} &= 1 + Y_n - aX_n^2 \\ Y_{n+1} &= bX_n \text{ where } n = 0, 1, 2 \dots \end{aligned} \tag{1}$$

Here, the parameters, a and b are of prime importance as the dynamic behavior of system depends on these values. The system cannot be chaotic unless the value of a and b are 1.4 and 0.3 respectively.

Step 4: This sequence is converted into [1 256] range using modular arithmetic.

$$\begin{aligned} X &\in \{-I, +I\}; \text{ Where } I \text{ is integer} \\ \text{New_} X &\leftarrow \text{floor}\{(256 \times X_{256})\} \\ \text{New_} X &\leftarrow \text{MOD}(\text{New_} X, 256) \end{aligned}$$

Step 5: remove duplicate numbers from the sequence and replace by those numbers with 0 frequency count in sequence list as shown in fig. 4.

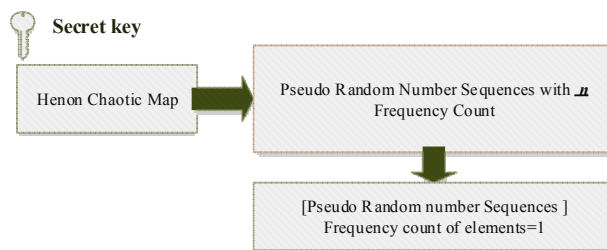


Fig.4:Pseudo random numbers for wire connections within Rotor

Step 7: Using the pseudo random sequence, labeling of output pins are done and wire are mapped with their corresponding label. This wiring of the model remains same until next setup.

Step 8: grayscale image is used as an input, where each pixel intensity is responsible for movement of fast rotor. Every pixel goes as input one by one into the system and gives output calculated by the below mentioned pseudo code for

encryption of image.

```

For I ← 1:M
For J ← 1: N
Ptr ← I (I, j) +1
For Rotor=1:3
    Number ← rotor (input pin, ptr)
    search (number1, rotor1) in output pin
    return index where number is found
end
Ref_idx ← mod(index[rotor3]+K7),256)
For Rotor ← 3:1
    search (number1, rotor) in input pin
    return index where number is found
end
end
end
end
    
```

Key Generation for Group B Members

Secret sharing scheme [20] basically splits the secret into shares and these shares are further distributed to the concerned group. Secret can be constructed only when group members participate to generate secret key. Here Shamir’s secret sharing (k, n) threshold scheme is used to split secret n members of the group. Therefore, parameters are taken as n=5, K=3 and P=17.

An equation is created with degree (K-1), and the coefficients (a₁, a₂) of the equation are chosen by group A members. Keystream is processed in secret sharing scheme and n shares of keystream’s size are distributed to the concern group. Where secret keystream is written in place of a₀.

$$f(x) = a_0 + a_1x + a_2x^2 \tag{2}$$

B. Decryption procedure

Group member can reconstruct a secret key using LaGrange interpolation method which is given below:

$$p(x) = \sum_{j=1}^n P_j(x)$$

$$\text{Where, } P_j(x) = Y_j \prod_{\substack{k=1 \\ k \neq j}}^n \frac{x - x_k}{x_j - x_k} \tag{3}$$

Step 3: At decryption end, users can generate keystream using (3) to reconstruct original image using the rotor machine.

EXPERIMENTAL RESULTS

In this section, experimental results of the proposed image encryption algorithm are given to appreciate the efficiency of proposed security system. MATLAB 7.9 software is used for implementation of proposed algorithm. Figure 11 shows PLP coefficients of voice sample (.wav format) used to generate keystream. Results of proposed system are shown in Fig.5-10 and table I.

Encryption process

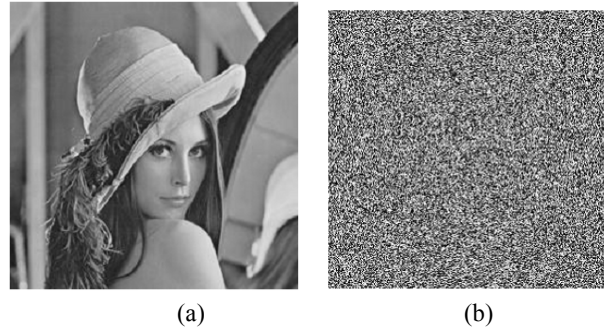


Fig.5.:Lena: (a) original image; (b) cipher image.

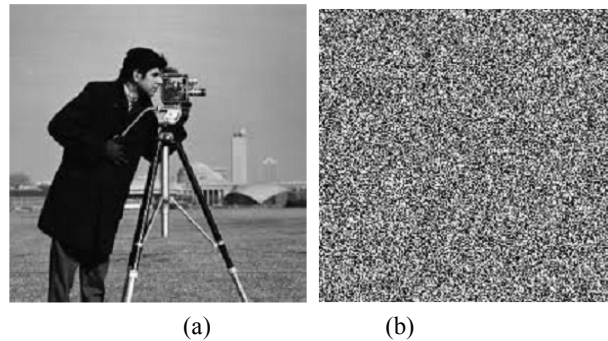


Fig.6: Cameraman: (a) original image; (b) cipher image

Decryption Process

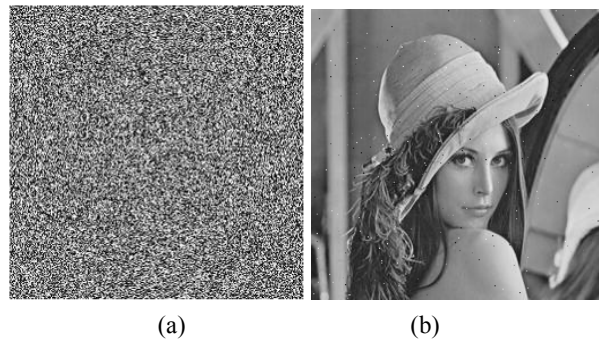


Fig.7:Lena: (a) cipher image; (b) decrypted image

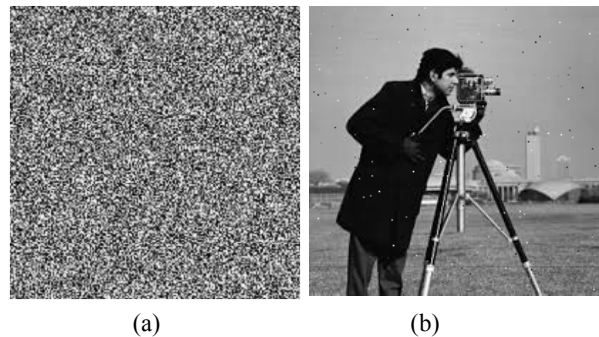


Fig.8: Cameraman: (a) cipher image; (b) decrypted image

Entropy Analysis of Results

Entropy of encrypted image decides ability of a cryptosystem which makes it difficult for eavesdropper to deduce information from cipher image. Ideal entropy of a

cryptosystem is $\cong 8$ which means uniform distribution of pixel values.

Histogram

Figure 9 shows uniform distribution of gray scale pixel values in cipher image, and significantly different from histogram of original image which proves that encrypted image does not help intruders to employ statistical attack on encryption procedure.

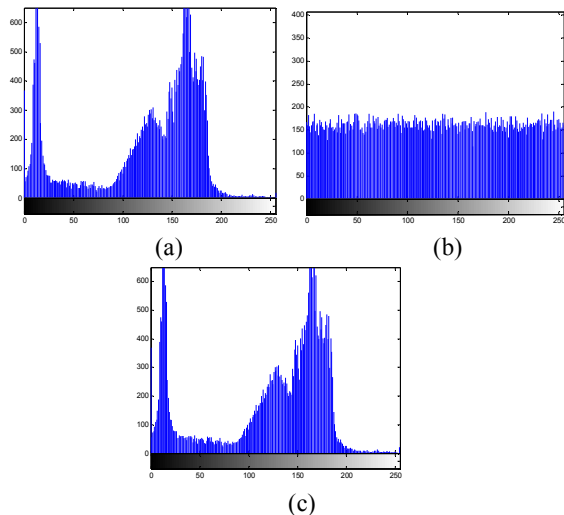


Fig.9.:Cameraman: (a) histogram of original image; (b) histogram of cipher image; (c) histogram of decrypted image

Table I: Entropy Analysis

Image name	Entropy of original image	Entropy of encrypted image
Cameraman.j pg	7.08601076783632	7.996133299611271
Lena.jpg	7.46687153562432	7.997155374413349

Mean Value Analysis

Mean value analysis gives average intensity of pixels in horizontal direction across the image. Mean value of cipher image in fig. 10 is shown by green color, which is consistent throughout. This indicates uniform distribution of gray levels whereas decrypted image and original image are shown by red and blue color respectively. Both the lines overlap each other which means original image is obtained by the group after decryption.

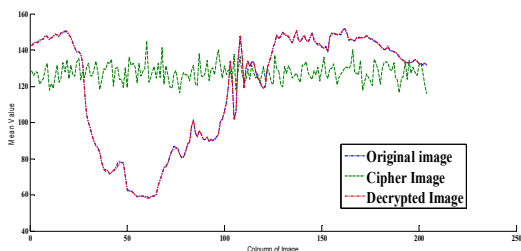


Fig.10: Cameraman: (a) original image; (b) cipher image

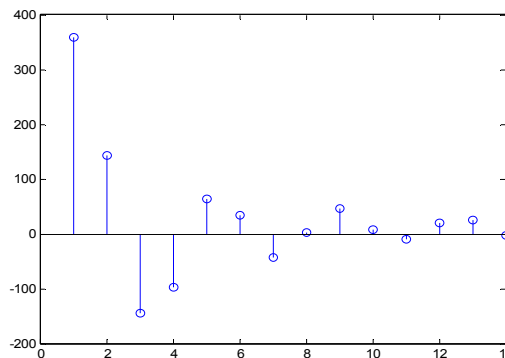


Fig.11. PLP coefficients of voice sample

CONCLUSION AND DISCUSSION

In this paper, property of electromagnetic machine is used with a novel approach to achieve confidentiality and authentication with high security. Speech is used as for authentication process and substitution cipher is achieved by electromagnetic machine which is based on the keystream and Hénon chaotic map. A system with three rotors will have 256^3 different combinations and same is followed in mapping of wires within rotor. Since chaos systems are very sensitive to initial condition so a slight change in initial key gives a different result and makes it impossible for intruder to break the cipher image. The proposed cryptosystem is applied on several test image and results show a high level of security given by system. For few test images, the decrypted images were found to have insignificant noise. Here, the security of system also relies on a speech signal along with the electromagnetic machine.

REFERENCES

Diffie, Whitfield, and Martin Hellman.1976. "New directions in cryptography." IEEE transactions on Information Theory **22:6**- 644-654.

G. Chen, Y. Mao, C.K. Chui,2004. "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos Solitons Fractals **21**:749-761.

S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan,2007. "A fast chaotic encryptions scheme based on piece wise nonlinear chaotic maps," Physics Letters, A, **366**:391–396.

Gaj, Kris, and Arkadiusz Orłowski.2003. "Facts and myths of enigma: Breaking stereotypes." International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg.

- Kruh, Louis, and Cipher Deavours.2002. "The commercial enigma: beginnings of machine cryptography." *Cryptologia* **26**: 1-16.
- <http://w1tp.com/4sale/>
- <http://users.telenet.be/d.rijmenants/pics>
- Fazel, Amin, and Shantanu Chakrabartty.2011. "An overview of statistical pattern recognition techniques for speaker verification." *IEEE Circuits and Systems Magazine* **11.2**: 62-81.
- Kinnunen, Tomi, and Haizhou Li,2010. "An overview of text-independent speaker recognition: From features to supervectors." *Speech communication* **52.1**:12-40.
- Z. I. Zhu, C. Bu, H. Li and H. Yu,2011. "A New Chaotic Encryption Scheme Based on Enigma Machine," 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications, Hangzhou,198-202.
- H. Elkamchouchi and A. M. Elshafee,2007. "REBC2, Rotor Enhanced Block Cipher 2," 2007 National Radio Science Conference, Cairo,1-7.doi: 10.1109/NRSC.2007.371401
- H. ElKamchouchi and A. ElShafee,2008. "URESC, Unbalanced Rotor Enhanced Symmetric Cipher," The 14th IEEE Mediterranean Electrotechnical Conference, Ajaccio,77-81.
- G. Chen, Y. Mao, K. Charles, 2004."A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solutions & Fractals*, 749-761.
- K. Wang, W. Pei,2005. "On the security of 3D Cat map based symmetric image encryption scheme," *Physics Letters A.*, 432-439.
- S.-M. Chang, M.-C. Li, W.-W. Lin,2009. "Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications," *Nonlinear Analysis*, 869-880.
- H. Lian-xi, L. Chuan-mu, L. Ming-xi,2007. "Combined image encryption algorithm based on diffusion mapped disorder and hyperchaotic systems," *Computer Applications*,1892-1895.
- Monrose, Fabian, et al. 2001."Cryptographic key generation from voice." *Security and Privacy*, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on. IEEE.
- Apte, Dr Shaila D.,2012. "Speech and audio processing." *WileyIndia*,109-125.
- N. S. Raghava, Ashish Kumar,2013." Image Encryption using Hénon Chaotic map with Byte Sequence", *IJCSEITR*,**3**:11-18.
- Thien, Chih-Ching, and Ja-Chen Lin.2002. "Secret image sharing." *Computers & Graphics* **26.5**:765-770.
- Wahyudi, Winda Astuti, and M. Syazilawati.2007. "Intelligent voice-based door access control system using adaptive-network-based fuzzy inference systems (ANFIS) for building security." *Journal of Computer Science* **3.5**:274-280.