Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. Engg. 54 (2013) 12598-12602

ISSN: 2229-712X

Secured medical image transmission using chaotic map

I. Bremnavas[1], B.Poorna[2] and I.Raja Mohamed[3]

[1]Faculty in Computer Applications, National Institute of Technology, Trichirappalli – 15.

[2]SSS Shasun Jain College for Women, T.Nagar, Chennai.

[3]Department of Physics, B.S.Abdul Rahman University, Vandalur, Chennai.

ARTICLE INFO

Article history:

Received: 16 November 2012;

Received in revised form:

15 January 2013;

Accepted: 18 January 2013;

Keywords

Encryption,
Decryption,
Chaotic Henon map,
Cryptography,
Steganography,
Information hiding.

ABSTRACT

Image cryptography and Steganography has attracted extensive research on the security of message that is to be transmitted in the open insecure medium. This is due to the fact that huge amounts of data can be hidden without perceptible impact to the carriers and possibly because of the popularity of electronic images and medical images that have become widely available. The chaotic based secret writing has its own advantage and it is mainly based on the initial condition which is the secret key for the secret writing. The chaotic based encryption serves as the robust mechanism against all sorts of attacks. In this paper, a novel image encryption and decryption scheme is proposed. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. Here a chaotic Henon map is used to generate permutation signal. Simulation results illustrate that the scheme is highly key sensitive and shows a good resistance against brute-force and statistical attacks.

1. Introduction

Along with the fast progression of data exchange in electronic way, it is important to protect the confidentiality of data from unauthorized access. Security breaches may affect user's privacy and reputation. So, data encryption is widely used to confirm security in open networks such as the internet. Due to the substantial increase in digital data transmission via internet, the security of digital images has become more prominent and attracted much attention in the digital world today. Many applications such as military database, medical image security, video conferencing etc., deserve the need of image security in order to keep the safe from the attackers. Also, the extension of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy and security for all applications. Each type of data has its own features; therefore, different techniques are used to protect confidential image data from unauthorized access.

Most of the available encryption algorithms are used for text data. However, due to large data size and real time requirement, the algorithms which are appropriate for textual data may not be suitable for multimedia data such as medical images. The algorithms which are followed for cryptography aren't suitable for encrypting the image since the size of the image is n times greater than the size of the secret text. Classical cryptographic algorithms such as RSA, DES, are inefficient for image encryption due to image inherent features, especially high volume image data. Traditional image encryption algorithms such as Data Encryption Standards [DES], Revest, Shamir, Adleman, [RSA] algorithm have the weakness of low level efficiency when the image is large. One-dimensional chaotic system with the advantages of high level efficiency and simplicity [1], such as logistic map, has been widely used now.

Their weakness, of assigning small key and weak security reduces their efficiency and performance [2,3]. Many researchers proposed different image encryption schemes to overcome image encryption problems [4,5,6,7,8].

2. Literature Survey:

Though a number of security algorithms have been proposed in the research areas, this algorithm is designed in such a way that it overcomes the disadvantages of the classical algorithms. In case of Bakers map based system proposed by Jolfaei has the disadvantage of shuffling the encryption key with the signal, the separation of the key with the image is difficult which causes major decryption problems and affects the clarity of the decrypted image. The novel encryption algorithm proposed by Xiqin gives the better results in case of gray scale image and it fails in its performance in colored and large scale images. The medical images are naturally larger in size and the size of the image to be encrypted is also unpredictable. Thereby the proposed work constitutes a novel algorithm to encrypt the image of any size and in a dynamic behavior. The Chaotic region is also a key in the proposed algorithm it serves as a better security and it reduces the time of decryption at the receiver's side. The performance of the proposed algorithm gives better results on comparing with the other security algorithm. The proposed algorithm by sud is single dimension in nature and a larger data cannot be encrypted using the single dimension logistic maps. An external key is required for the decryption algorithm which delays the decrypting time and causes inability to perform incase of single dimension.

3. Effectiveness in the Proposed Work:

This research tries to find a simple, fast and secure algorithm for image encryption using the characteristics of chaotic functions. Due to larger key's space in the chaotic functions, this method is very robust. The real robustness in

Tele:
E-mail addresses: jmcnavas@gmail.com

chaotic based image encryption lies in choosing the better chaotic attractor. Though a large list of chaotic map has beendeveloped, logistic chaotic maps are single dimension and it is inefficient to provide the security using the single dimension for a large amount of data. The Henon map overcomes this problem since it is two dimensional in nature and itself is a pseudo random generator.

The rest of the paper is organized as follows: In Section 2, Literature Survey regarding many numbers of past works is explained, Section 3 Effectiveness in the proposed work is explained, Section 4 explains relation between Chaotic System. Section 5, briefly explains the Semantic diagram of the system used in this paper. In Section 6 the proposed sender side and receiver side algorithm is also discussed. Section 7 describes Analysis and Test Results. In Section 8 the future work is given. Finally, some Conclusions are given in section 9 and References section is 10.

4. Chaotic System:

The Study of nonlinear dynamical and chaotic systems over the past decade has led many researchers to reconsider what is meant by "noise". In many cases, the deterministic signal from a nonlinear system may look like noise when displayed in either the time or the frequency domain. Much of the engineering work in this area has involved a search for applications of these noise-like deterministic signals. This property has been used in spread spectrum communications by replacing the pseudo-random sequences with chaotic signals.

The chaotic signals are like noise signals but they are completely certain, that is if we have the primary quantities and the drawn function, the exact amount will be reproduced.

4.4.1. Chaotic Henon Map:

The Henon map is a prototypical two dimensional invertible iterated map represented by the state equations with a chaotic attractor and is a simplified model of the Poincare map for the Lorenz equation proposed by Henon in 1976 [9]. The chaotic Henon mapping has been proposed as a method of generating pseudo-random sequences [10]. The two-dimensional Henon map is defined as follows:

$X_{n+1} = 1 + y_n - \alpha x_n^2$ --------- (1)

$Y_{n+1} = \beta x_n$ -------- (2)

Where 'α' and 'β' are constants. With initial point (x_0, y_0). The pair (x, y) is the two dimensional state of the system. When $\alpha = 1.4$ and $\beta = 0.3$, the system is in chaotic state. Henon showed that if the initial point lies in the area S defined by the four points (-1.33, 0.42), (1.32,0.133), (1.245, -0.14) and (-1.06, -0.5), then the subsequent points, (x_i, y_i) for $i \geq 1$, also lie in S. The Henon map possesses a strange attractor. For any values of (x_i, y_i) in S, the sequence of points quickly converges to this attractor and remains on it during the iterations that follow. [11,12]

Implementation:

First step in this work is to generate the noisy signal using the Chaotic Henon discrete equations 1 and 2. The user sets the cover region dynamically by setting value for control parameters α and β. The input patient medical image data has been taken. Here the Henon equations are generated with the signal in both 'x' and 'y' axes. The advantage of using the Henon map is to send two patient medical images at a single transmission. For example if it is required to send two patient medical images in one transmission, the first patient medical is added in 'x' axis and then another one is added in 'y' axis. Both the patient medical images are arranged in one dimensional array format. The Henon pixel data and patient medical image pixel data are embedded and the process started with the key value α = 1.4 and β=0.3. So, both data are stored in any location in the cover region.

Any intruders need to hack that encrypted data, since only the cover boundary is visible. The intruders could not understand whether any text data or image data is there, otherwise for the hackers to understand it is a plain boundary. In case of the intruders knowing any information hidden inside the cover region, he is not hacking the encrypted data, because he doesn't know the key value. Here, the advantage of this work is, generated pixel data fully is in the cover region, and then the initial key 1.4 in 'x' axis and 0.3 in 'y' axis or any dynamically selected key by the user is taken.

Between the values 0 to 1.4 in 'x' axis 0 to 0.3 in y' axis, there is no encrypted data. After the key value 1.4 and 0.3, the encrypted data is present. So, there are two extreme levels. It is not possible for the intruders to hack the information. The hackers could get the signal and the time of decoding the signal without the knowledge of initial value that could take decades to solve the puzzle.

5.Semantic Diagram

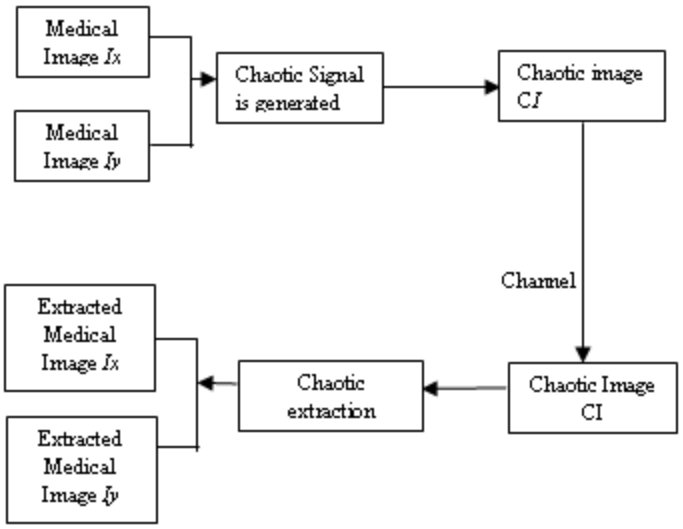

Figure 1. Flow Diagram for secured medical image transformation using Chaotic Henon Map

The Fig. 1 describes the encryption scheme. The chaotic sequence is generated and the image is converted into pixel array, the image signal is encrypted in the chaotic region using a summer for better security purpose a noise signal can be generated and it can be added in order to increase the complexity of the attackers. The addition of the noise signal is only optional. Now the encrypted signal with or without noise is being sent through the open communication channel. The receiver side follows the same procedure and decrypts the user image. If at all noise is added in the sender side the mathematical treatment is done in order to eliminate the noise in the receiver side. Addition of noise with the input signal is only optional based nature of insecure area.

6. Proposed Algorithm:

Proposed Embedding Algorithm

I/P : Medical Images Ix, Iy

O/P : Encrypted signal, ES

Step 1 : Load an Image for each x and y co-ordinates and represent in a one-dimensional array named Ix and Iy.

Step 2: Generate the Chaotic Signal S using Henon Equation

$X_{n+1} = 1 + y_n - \alpha x_n^2$ ---- (1)

$Y_{n+1} = \beta x_n$ ---- (2)

Step 3: The Image Ix is embedded within the Chaotic Signal S using the following steps

3.1. Fixed the covered Boundary Region based on the size of an Image Ix.

3.2. The Signal is assumed to be generated from the starting position of the

Boundary Region

3.3. Set a key value K dynamically within the boundary region to represent the initial position.

3.4. The Image value Ix is embedded with Chaotic Signal S from K.

Step 4: The step 3 is repeated for the Image Iy with the same key value, K.

Step 5: The Encrypted signal (ES) is transferred along the key value K. (The key value is embedded in a standardized position of the signal ES).

Proposed Extraction algorithm

The encrypted image is received by the trusted source. The key is also embedded in the same cover region. The receiver generates the random numbers using same Henon equation called raw Henon. The encrypted Henon map is subtracted from the raw Henon map thereby the image is being retrieved from the encrypted source of information.

I/P: Encrypted signal, ES

O/P: Medical Images, Ix and Iy

Step 1: Receive the encrypted signal, ES from the open communication channel.

Step 2: Retrieve the key value K from Encrypted Signal ES.

Step 3: Generate the Chaotic Signal S using Henon Equation

$X_{n+1} = 1 + y_n - \alpha x_n^2$

$Y_{n+1} = \beta x_n$

Step 4: Subtract the received encrypted signal, ES with the raw Henon signal, S using the key value K, to obtain a one-dimensional array for each medical image Ix and Iy.

Step 5: Construct the resultant images Ix and Iy from the one-dimensional array.

Model Simulink Diagram

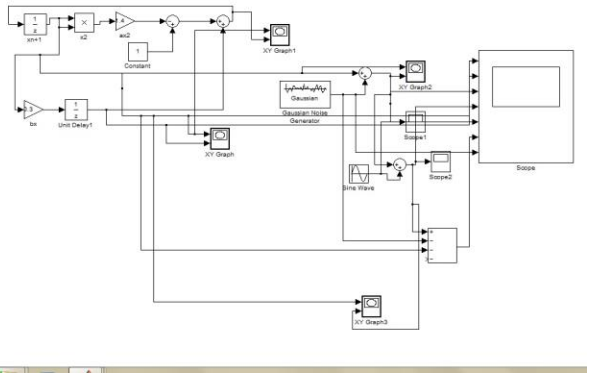

Fig 2: Matlab Simulink diagram with Gaussian noise

Fig 2 describes the basic chaotic generator using matlab Simulink process, in the Simulink module the Henon equation is simulated and the results are shown for various chaotic region Fig 3 describes the change in the raw chaotic map for different chaotic region. Thereby the robustness for the chaotic map is observed. The chaotic region is mainly based on the initial value taken and thus the initial value of the Henon attractor serves as the key for the image encryption process.

Here the Simulink model is designed, based on the Henon Map equations. These Simulink Model is to generate the signal. Aim of our work is to impose the image on the signal.

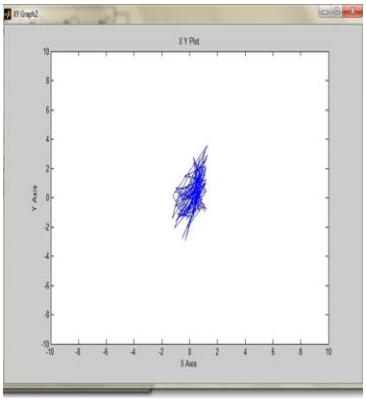

Fig 3: Henon sequence within the area -2 to 2

Fig 3 describes the chaotic map with the region of -2 to 2 with the initial condition of 0.3 in x axis. The sequence is generated with the two dimensional signal the plot with respect to x axis and y axis. The Simulink Model is generated by different wave form. The figure illustrates different level of signal phases and waveform for different initial values and different regions of the chaotic region. The initial value and chaotic region is the major challenge faced by the attackers in decrypting process of the user data. A wrong initializing value can make the attractor to converge and will give a wrong sequence through which the decryption process cannot be done.

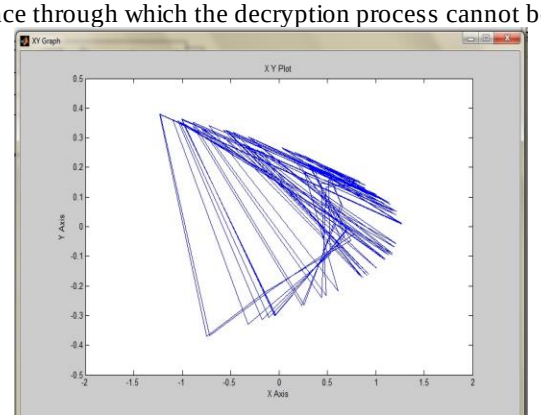

Fig 4: Henon sequence between -0.5 to 0.5

Fig 4 describes the Henon sequence within the area of -1.5 to 1.5 with the initial condition of 0.5 and the plot is plotted with x axis with respect to y axis, from Fig 3 and Fig. 4 the difference in sequence plot and their difference in the initial conditions are shown. The robustness of the Henon is clear from the plots depicting above the change in plot with the change in initial condition and with change in the area of the chaotic sequence. The 3 plots could be obtained using the Henon equation X versus A, Y versus A, X versus Y plots are obtained among which X versus Y is the two dimensional in nature.

7.Analysis and Test Results:

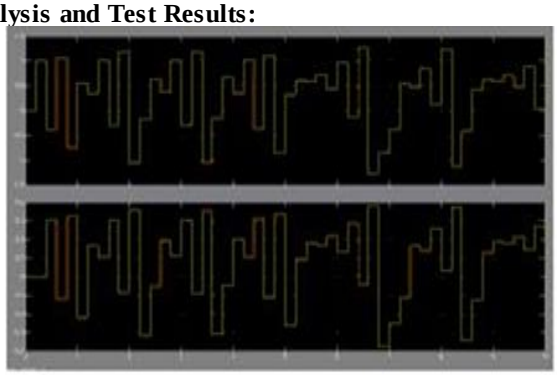

Fig. 5. Time Series of System Variables x and y

Fig 5 illustrates the dynamic behavior of the chaotic sequence, the wavelength of the chaotic signal varies with different initial conditions.

Based on the Henon map equations the generated signal is plotted as a graph.

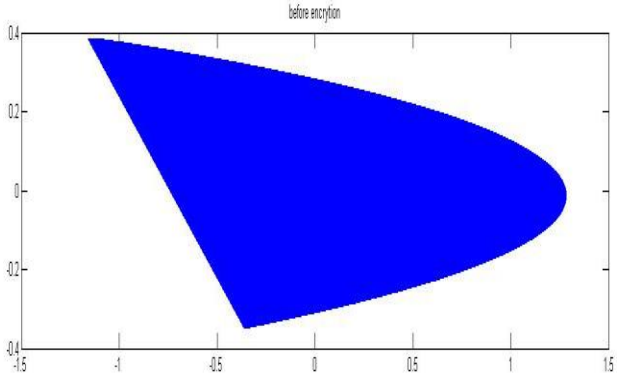

Fig. 6. depicts the phase filled henon map in which the chaotic regions is shown in the raw chaotic map generated through the matlab simulator.

Fig 6 shows the shows the raw henon sequence with -1.5 to 1.5 with 0.4 as the initial condition as taken as the signal for embedding the image signal the fig 6 is the XY plot.

The original medical image (fig. 7) is placed in the top phase of henon map then the medical image is encrypted.

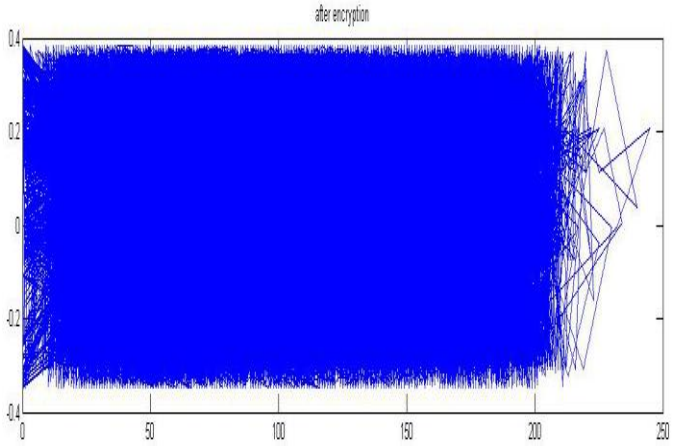

Fig. 7. signal after encryption.

Fig 7 shows the encrypted chaotic sequence alone apart from other values the XY plot of Fig 7 is addition of chaotic sequence and image signal. The medical image is encrypted and also it is covered. Medical images of the patient to be encrypted.

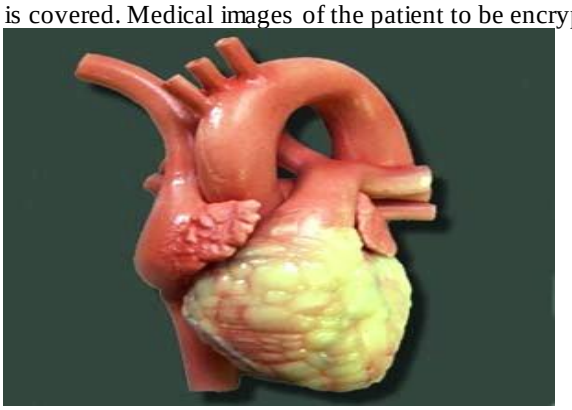

Fig. 8. Image before Encryption

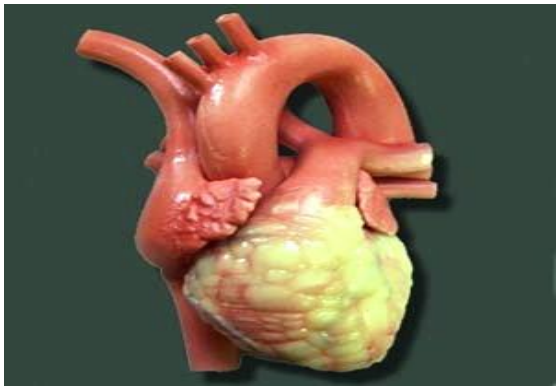

Fig. 9. Image after Decryption

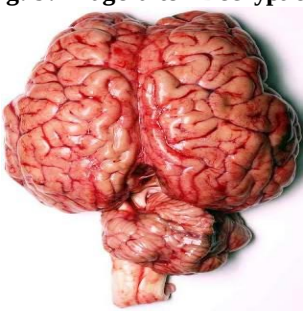

Fig 10. Image before Encryption

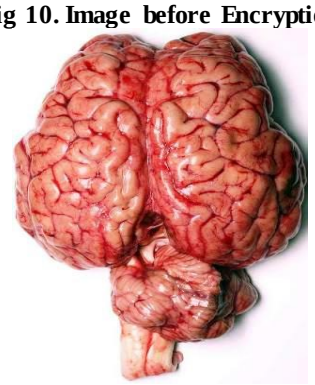

Fig.11. Image after Decryption

A heart image of size 300*300 and a brain image of 315*448 is used as the image signal and it is encrypted both with the noise and without noise signals and decrypted using the Henon sequence. The medical images of heart and brain of different size is used. The algorithm works for various sizes of medical images. In the decryption phase, the receiver receives the encrypted medical image and filters the chaotic signal.

8. Future Work:

The algorithm can be implemented for more image encryptions and with three dimensional sequence data. The algorithm could be tested with various images with more size and three dimensional images. This algorithm works efficiently for single image in two dimensional equations. This can be extended for more images with the same two dimensional equations.

9. Conclusion:

In this paper, an encryption and decryption scheme has been presented. A chaotic map is used to generate a permutation matrix with two variables to build shuffler. Henon map is a good candidate for permutation matrix generation. All parts of the proposed chaotic encryption and decryption system were simulated using MATLAB SIMULINK and MATLAB Programming. The proposed schemes key space is large enough to resist all kinds of brute-force attacks. The differential analysis results illustrate that a small change in the original image will

result in a negligible change in the decrypted image. The theoretical and Simulink results show that the proposed encryption and decryption scheme can be a potential candidate for image processing for cryptography and steganography.

10. References:

[1] Elnashaie SSEH, Abasha ME. On the chaotic behaviour of forced fluidized bed catalytic reactors. Chaos, Solitons & Fractals 1995; 5:797–831.

[2] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circ Syst 2001; 1:6–21.

[3] Ponomarenko VI, Prokhorov MD. Extracting information masked by the chaotic signal of a time-delay system. Phys Rev E 2002; 66:026215–21.

[4] M. Sharma and M.K. Kowar, "Image Encryption Techniques Using Chaotic Schemes: a Review," *International Journal of Engineering Science and Technology*, vol. 2, no. 6, 2010, pp. 2359–2363.

[5] A. Jolfaei and A. Mirghadri, "An Applied Imagery Encryption Algorithm Based on Shuffling and Baker's Map," *Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR-10)*, Florida, USA, 2010, pp. 279–285.

[6] A. Jolfaei and A. Mirghadri, "A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1," *Proceedings of The 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10)*, Sanya, China, 2010.

[7] L. Xiangdong, Z. Junxing, Z. Jinhai, and H. Xiqin, "Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 1, 2008, pp. 64–68.

[8] N.K.Pareek, Vinod Patidar,K.K.Sud,"Image encryption using chaotic logistic map", Image and Vision Computing , Elsiever,pp 926-934, 2006.

[9] M. Henon, "A Two-Dimensional Mapping with a Strange Attractor," *Communication in Mathematical physics*, vol. 50, 1976, pp. 69–77.

[10] R. Forre, "The Henon Attractor as Key Stream Generator," *Abstracts of Eurocrypt 91*, 1991, pp. 76–80.

[11] A.S. Alghamdi, H. Ullah, M. Mahmud, and M.K. Khan, "Bio-Chaotic Stream Cipher- Based Iris Image Encryption," *Proceedings of the International Conference on Computational Science and Engineering*, 2009, pp. 739–744.

[12] X.Y. Yu, J. Zhang, H.E. Ren, G.S. Xu1, and X.Y. Luo, "Chaotic Image Scrambling Algorithm Based on S-DES," *Journal of Physics: Conference Series*, vol. 48, 2006, pp. 349–353.