Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Securing Medical Images and Patient Data using Non-Linear Sequences

Mahalinga V. Mandi[1], Anand H. D.[2]

[1]Department of Electronics & Communication Engineering,
Dr. Ambedkar Institute of Technology, Bangalore, India
mvmandi.ec@drait.edu.in
[2]Department of Electronics & Communication Engineering,
Dr. Ambedkar Institute of Technology, Bangalore, India
anandhd.ec@drait.edu.in

Article History:

Received: 14-01-2025

Revised: 15-02-2025

Accepted: 21-03-2025

Abstract:

Hiding of patient data in medical image along with image encryption is a growing research area. The use of chaos in image watermarking and image encryption algorithms has seen tremendous advantages. In this paper a chaos-based image watermarking to provide authentication and chaos based watermarked image encryption algorithm to provide security is presented. The performance of the image watermarking and encryption is mainly based on the chaotic logistic map equation. In order for a complex imaging system to cope with these concerns, a cryptography algorithm able to manage the vast amounts of data involved in image processing is required. This paper proposes a new image watermarked encryption method using one-dimensional chaotic map namely Logistic map equation. Using this algorithm, the key space is enlarged to 2212 to improve the security against exhaustive attacks, and also a good encryption speed can be achieved. The results of the proposed method show that it is more efficient interms of key space, entropy and key sensitivity properties.

Key Words: Watermarking, Image encryption, Logistic map, Chaos

1. Introduction

The growth of the digital technology and the associated need for information integrity, authenticity and secrecy encourages the development of secure image encryption systems. After the advent of the Internet and especially nowadays, security of data and protection of privacy has become a major concern for everyone's life. Combining the properties of cryptography and chaos theory it is possible to design an image encryption algorithm that provides security, authentication and privacy in image and video applications. Cryptography deals with watermarking techniques to provide authentication and encryption techniques to provide security. Chaos theory provides the suitable non-linear binary sequences that can be applied to watermarking and encryption algorithm.

Chaos is a deterministic, random like process found in non-linear, dynamical system which is non-periodic, non-converging and bounded. Chaotic signals are random like but they are produced by deterministic systems and can be reproduced. Chaotic systems are sensitive to initial conditions and thus even with a small difference in initial conditions will lead to the generation of very different signals from the same dynamical system. The inherent properties of chaotic functions are suitable for

generating key stream for watermark and encryption algorithm. Chaotic sequences are non-repeatable, if only part of the sequence is recovered then it is nearly impossible to regenerate the whole sequence. This implies that any inadvertent receiver exposed to these sequences will see waveforms that resemble noise and lack any characteristics that could be used to intercept signals.

The chaos-based image watermarking and encryption is discussed in [1] – [15]. A watermarking procedure for digital image in the Complex Wavelet Domain is discussed in [1]. The proposed watermark algorithm needs three keys: a sub image, a random location matrix and spread spectrum watermark. The first and the second ones ensure the security of watermarking procedure and the third one guarantees its robustness.

A watermarking method using chaotic function and a correlation is discussed in [2]. This method is compared with existing methods and found to be better.

Paper [3] discusses a digital watermarking technique based on chaos theory and DWT. DWT is used to extract the low frequency signals and then the sequences are generated using Chaotic function are used for encryption of watermark.

An efficient, secure colour image coder incorporating Colour-SPIHT (C-SPIHT) compression and encryption (partial) is presented in [4]. By encrypting only the LSB of each individual wavelet coefficient for K iterations of the C-SPIHT method, it is demonstrated here that the image data is secure. By varying K, the level of confidentiality vs. processing overhead can be controlled.

An image security method using chaotic logistic maps for transfer of image securely is discussed in [5]. Here an 80bit key with two logistic maps are utilised.

An image encryption method using four chaotic array is discussed in [6] and uses chaotic maps to generate four valued chaotic array whose size as big as image.

An image encryption cryptosystem by combining two chaotic maps is presented in [7]. The permutation is done using cat map and the substitution is performed using one-way coupled map lattice (OCML).

In paper [8], using chaotic functions namely Chen hyper-chaotic map, logistic map and Arnold map are used for encryption for applications in cellular automata.

A two-phase encryption method using two-chaotic functions namely Logistic map and Arnold map for protecting grey scale images is discussed in [9].

In paper [10], the encryption of colour images using chaotic map and block scrambling is discussed.

Image encryption of colour images using hash function and chaotic Lorenz map is presented in [11].

In paper [12], a method for securing image using hyper-chaos is discussed and found to be more secure as it uses permutation in pixel and bit level.

The concept of bijective function using substitution box derived from Chen system for encryption of colour image is presented in [13].

In [14], an encryption technique for colour images is introduced using Global Bit Scrambling (GBS) and Integer Wavelet Transform (IWT) techniques.

In paper [15], it is demonstrated that using arrangement of pixel and random permutation to secure medical images improves security while enabling fast encryption.

Organization of the paper is as follows. Section 2 discusses the objectives of proposed work. Section 3 presents architecture of proposed method. Experimental results are discussed in Section 4. Finally, the discussion on the advantages of proposed algorithm is highlighted in Section 5.

2. Objectives

This paper proposes a new watermarked image encryption technique based on chaos. The first stage involves embedding patient data (a watermark) into the cover image. Two additional procedures are then used to encrypt the image. The image is first position permuted and each pixel is then XORed to complete the substitution. The chaotic logistic map equation is used to determine the necessary keys..

3. Architecture of Proposed Method

Figure 1 displays the schematic of the suggested non-linear image encryption technique with an incorporated watermark. Fig. 1 is divided into two halves. In the first section, use LSB insertion to embed the watermark in the plain image. In the second portion, use the chaotic logistic map equation to encrypt the watermarked image. The LSB keystream is obtained using the non-linear chaotic logistic map equation and LSB insertion is carried out at random.

All the keys are generated on DSP Embedded Evaluation Board TMS320C6748 Series. Code Composer Studio (CCS), version 12.0, and Visual Studio C++, version 6.0, were the software tools utilized during development. After being created in Visual Studio, the chaotic generator's C code was transferred to CCS, built, and optimized before being downloaded to the TMS320C6748 DSP.

Using LSB insertion method a large watermark can be embedded when compared with other methods. In the watermarked image encryption, mainly two steps are involved. In order to create an encrypted image, the image is first position permuted and then each pixel is bitwise XORed with Key 3. The Key 1 is utilised for row permutation and Key 2 is utilised for column permutation.

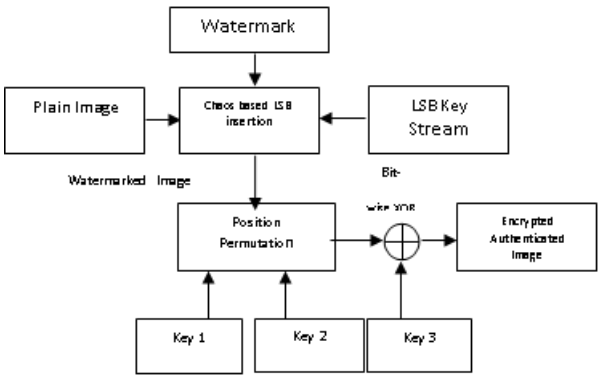

Figure 1. Proposed Encryption Scheme

Figure 2 shows the patient data extraction from the medical image. Here the decryption of the patient data embedded in medical image is exactly the reverse process and the same Key streams are used.

The patient data is also extracted with the same LSB Key stream. By comparing the retrieved patient data with the reference patient data, it is also feasible to determine whether the patient data has been altered or tampered with. As a result, the suggested algorithm offers both the authentication and the necessary security.

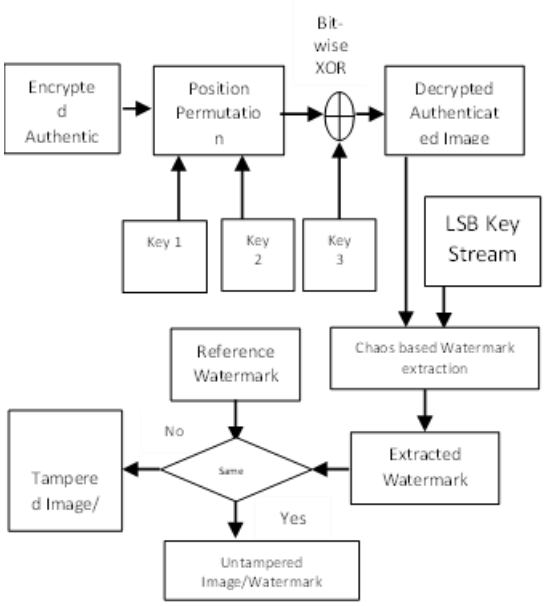

Figure 2. Watermark Detection

2.1. Key stream generator

Figure 3 shows the bock diagram for deriving key sequences. Using Logistic map [16] given in Equation (1), discrete sequences are derived first by considering an initial value.

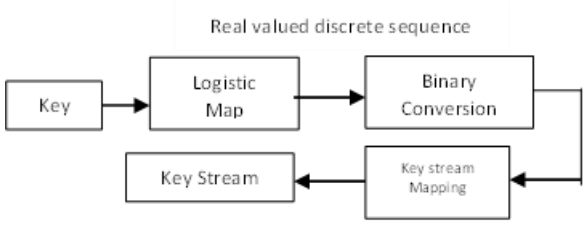

Figure 3. Key Stream Generation

$$x_{k+1} = r * x_k * (1- x_k), \ 0 < x < 1 \qquad (1)$$

where initial value is x0 and bifurcation parameter is r. By varying these two values x0 and r, it possible to generate different non-linear sequences of any length. It is observed that, for $3.57 < r \leq 4$, the sequences exhibit chaotic behaviour [17]. To convert these sequences which are discrete to binary, a simple threshold function is used as shown in Equation (2).

$$bi = 0 \text{ for } xk < 0.5$$

$$\text{and } bi = 1 \text{ for } xk \geq 0.5 \qquad (2)$$

where $0 < i < n$ and n is the sequence length.

Three sub-keys make up Key = {key1, key2, key3}, where sub-key1 serves as the starting value for key 1 generation, sub-key2 serves as the starting value for key 2 generation, and sub-key3 serves as the starting value for key 3 generation.

2.2. Key Stream Mapping

Figure 4 displays the key stream mapping used to generate keys 1, 2, and 3.

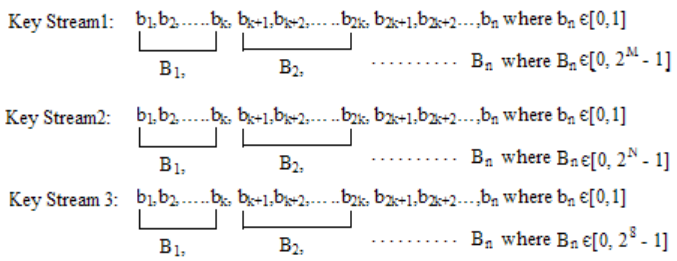

Figure 4. Key Stream Mapping

For each stream, the decimal numbers B1, B2,..., etc., are the result of mixing k-binary numbers. The length of key 1 (used for row permutation) must be 2^M with a range of $[0, 2^{M-1}]$, key 2 (used for column permutation) must be 2^N with a range of $[0, 2^{N-1}]$, and key 3 (used for bitwise XORring) must be 2^M X 2^N X 8 with a range of [0, 255], assuming that the cover image is of size 2^M X 2^N.

Duplicate elements in the two streams, if any, will be eliminated during the creation of keys 1 and 2, meaning that the repetitive sequence is eliminated.

Like key 3, the LSB key stream mostly relies on the watermark's size.

4. Results

In order to test this algorithm a standard 512 X 512 medical image is considered. In this medical image the patient data is embedded. The initial values are randomly selected as key = {key1, key2, key3} = {0.32414432, 0.59874561, 0.86524416}, with the value of "r" being set at 3.99. The seed value for creating the LSB key stream is 0.62343242.

Figure 5 shows the 512 X 512 patient medical image and patient data of 362 characters which is to be embedded. Each character is represented by 8 bits which results in 2896 bits and is embedded randomly in the medical image. It is possible to embed about 262144 bits which is almost equal to 32768 characters of patient data.

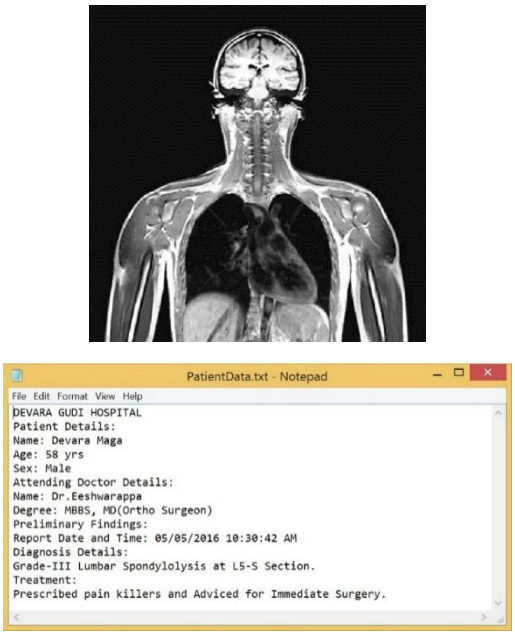

Figure 5. Patient Medical Image and Patient Data to be Embedded

The histograms of the input medical image, encrypted image, encrypted image histogram, and decrypted image are displayed in Figures 6 through 9, respectively.

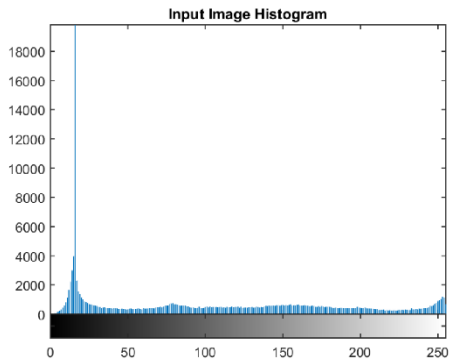

Figure 6. Input Medical Image Histogram

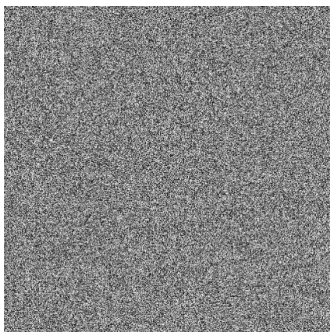

Figure 7. Encrypted Image

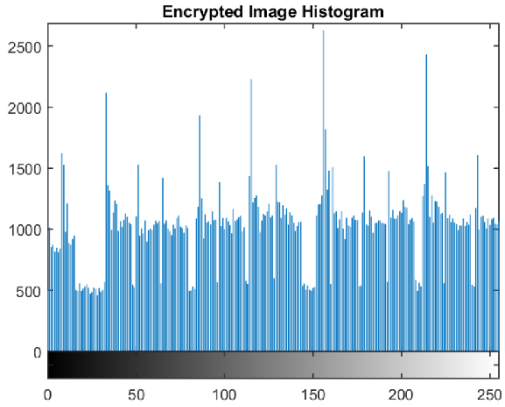

Figure 8. Encrypted Image Histogram

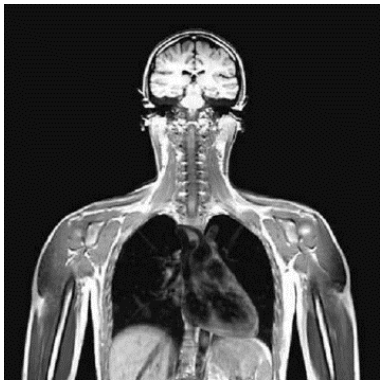

Figure 9. Decrypted Image

The encryption and Decryption time in Matlab for a 512 X 512 BMP medical image was found to be 0.015625 seconds.

5. Discussion

A strong encryption method should withstand all known assaults, including brute force attacks, ciphertext-only attacks, known/chosen plain text attacks, and statistical attacks. This section presents the security analysis of the suggested encryption system.

5.1. Key Space Analysis

The most popular PC platform, for instance, has a computation precision of 16 decimal digits. As a result, a chaos-based cryptosystem can only offer a key space of 1016≈253 [18], which is significantly smaller than AES (2128) and somewhat smaller than DES (256). Because key = {key1, key2, key3} and LSB key, which is composed of four sub-keys, the key space size is (1016)4 ≈ 2212, which is larger than the most secure AES algorithm. Additionally, because the method uses both permutation and substitution operations, it is safe from known/chosen-plaintext attacks.

5.2. Information Entropy

For an image, each pixel is of 8-bit, the ideal value of entropy is eight [19]. The input medical image's entropy is 2.030734, while the encrypted image's entropy is 7.93041, which is quite close to the theoretical value of 8. The suggested scheme's encrypted image's entropy is quite near to the optimal value. Additionally, the watermarked image's entropy is 2.040747, nearly identical to the input images.

5.3. Key Sensitivity

A decent cryptosystem should be sensitive enough to even slight changes in key. The image cannot be decrypted in the suggested scheme with a slight alteration to the key. This was observed by choosing the key = {0.32414432001, 0.59874561, 0.86524416} and using the incorrect key to decrypt the image. Only key1 is slightly changed to 0.32414432001 instead of the correct key1=0.32414432, and it is observed that decryption is totally impossible. Figure 10 shows the decrypted image with the wrong key along with the corresponding histogram. The medical image that was decoded with the wrong key has an entropy of 7.931566.

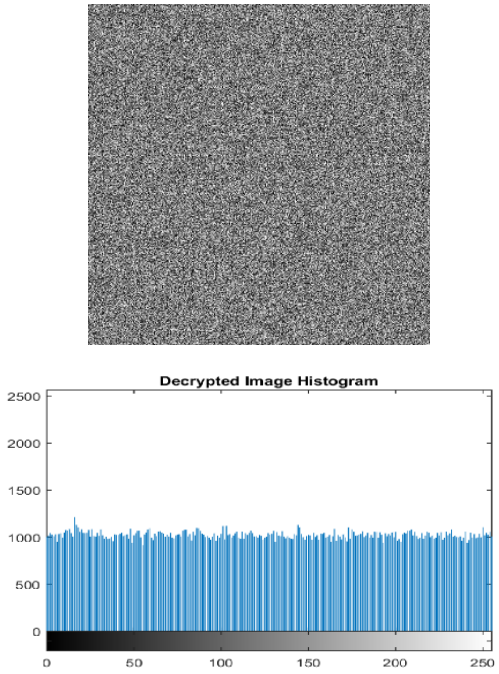

Figure 10. Decrypted Medical image and its histogram with a wrong key

Additionally, it has been noted that using the incorrect key to retrieve patient data produces some trash characters, as seen in Figure 11.

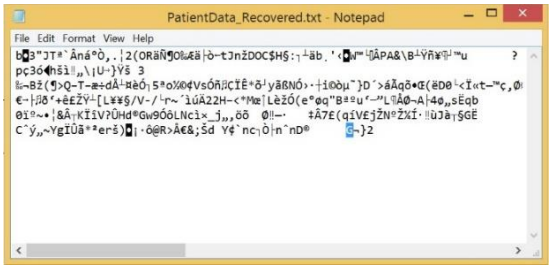

Figure 11. Extracted Patient Data with a Wrong Key

This research proposes an excellent performance chaos-based method for encrypting and embedding patient data for medical images. This study suggests an algorithm that provides both security and authenticity. This technique has the advantage of having a larger key space (2212), which increases security against exhaustive attacks. It also has a good encryption speed, which improves performance when the image size is huge. The histogram of the encrypted image shows that the entropy is very close to the ideal one, which makes the image appear to be quite random. Based on simulation results, the proposed method delivers good security for medical images and has outstanding key sensitivity. Additionally, this approach can be expanded to secure other multimedia data, including messages, audio and video.

Acknowledgement

The Karnataka government's Vision Group of Science and Technology (VGST) provided funding and assistance for this effort through K-FIST (L1) awards. The authors would like to express their gratitude to VGST and the Management, PVPWT for carrying out the project at Dr. Ambedkar Institute of Technology, Bengaluru.

References

[1] S. Mabtoul, E. Ibn-Elhaj, D. Aboutajdine, “A Blind Chaos-Based Complex Wavelet-Domain Image Watermarking Technique”, Proc. Int Jnl. of Computer Science and Network Security, Vol.6, No.3, pp. 134-139, March 2006.

[2] E. Chrysochos, V. Fotopoulos, and A. N. Skodras, “Robust Watermarking of Digital Images Based on Chaotic Mapping and DCT”.

[3] Qiang Wang, Qun Ding, Zhong Zhang and Lina Ding, “Digital Image Encryption Research Based on DWT and Chaos”, Proc. Fourth IEEE Int. Conf. on Natural Computation, pp. 494-498, 2008.

[4] Karl Martin, Rastislav Lukac, Konstantinos N. Plataniotis, “Efficient encryption of wavelet-based coded color images”, Jnl. Pattern Recognition Society, Elsevier, pp. 1111 – 1115, 2006.

[5] N.K. Pareek, Vinod Patidar, and K.K. Sud, “Image encryption using chaotic logistic map”, Jnl. Image and Vision Computing, Elsevier, pp. 926–934, 2006.

[6] Gao Shan-qing, Zhang Shi-jie, Liu Bin, Luo Xiang-yang and Liu Fen-lin”, An Image Encryption Algorithm based on Four-value Chaotic Array”, Jnl. Image and Graphics, Vol. II, No. 2, pp. 244-250, Feb. 2006.

[7] Zhang YiWei1, Wang YuMin & Shen XuBang, “A chaos-based image encryption algorithm using alternate structure”, Springer, Vol. 50, No. 3, pp. 334-341, June 2007.

[8] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, ‘‘Color image encryption based on hybrid hyper-chaotic system and cellular automata,’’ Opt. Lasers Eng., vol. 90, pp. 225–237, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.019.

[9] D. Zareai, M. Balafar, and M. Feizi Derakhshi, ‘‘EGPIECLMAC: Efficient grayscale privacy image encryption with chaos logistics maps and Arnold Cat,’’ Evolving Syst., vol. 2023, pp. 1–31, Jan. 2023, doi: 10.1007/s12530-022-09482-w.

[10] K. M. Hosny, S. T. Kamal, and M. M. Darwish, ‘‘A color image encryption technique using block scrambling and chaos”, Multimedia Tools Appl., vol. 81, no. 1, pp. 505–525, Jan. 2022, doi: 10.1007/s11042-021-11384-z.

[11] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, ‘‘A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2,’’ Optik, vol. 159, pp. 348–367, Apr. 2018, doi: 10.1016/j.ijleo.2018.01.064.

[12] Y. Li, C. Wang, and H. Chen, ‘‘A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, ’Opt. Lasers Eng., vol. 90, pp. 238–246, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.020.

[13] H. Liu, A. Kadir, and Y. Niu, ‘‘Chaos-based color image block encryption scheme using S-box,’’ AEU Int. J. Electron. Commun., vol. 68, no. 7, pp. 676–686, Jul. 2014, doi: 10.1016/j.aeue.2014.02.002.

[14] J. Karmakar and M. K. Mandal, ‘‘Chaos-based image encryption using integer wavelet transform,’’ in Proc. 7th Int. Conf. Signal Process. Integr. Networks, Feb. 2020, pp. 756–760, doi: 10.1109/SPIN48934.2020.9071316.

[15] Koredianto Usman, Hiroshi Juzoji, Isao Nakajima, Soegijardjo Soegidjoko, Mohamad Ramdhani, Toshihiro Hori and Seiji Igi, “Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security”, IEEE, pp. 244-247, 2007.

[16] May, Robert M. Simple mathematical models with very complicated dynamics. Nature, Vol. 261, June 10, 1976.

[17] Mahalinga V. Mandi, R. Murali, K.N.Haribhat”, Chaotic functions for generating binary sequences and their suitability in Multiple Access, Proc. IEEE-ICCT 2006,Vol. 1,pp.217-220.

[18] Chong Fu, Zhiliang Zhu,” A Chaotic Image encryption scheme based on circular bit shift method”, The 9th International Conference for Young Computer Scientists, IEEE Computer Society, pp. 3057 – 3061, 2008.

[19] Xu Shu-Jiang, Wang Ying-Long, Wang Ji-Zhi, Tian Min,” A Novel Image Encryption Scheme Based on Chaotic Maps”, Proc. IEEE-ICSP 2008, pp. 1014 – 1018.