Journal of Computer Science and Software Development
Received: Oct 14, 2015, Accepted: Oct 21, 2015, Published: Oct 24, 2015
J Comput Sci Softw Dev, Volume 1, Issue 1
http://crescopublications.org/jcssd/jcssd-1-001.pdf
Article Number: JCSSD-1-001

Research Article **Open Access**

An Active Algorithm to Gray-scale Digital Image Forgery Detection based on Cellular Automata and LU Decomposition

Mohammad Amin MoghaddasiFar[1*], Faezeh Rohani[1*] and E Behravesh[2]

[1]Department of Computer Science, Sanabad Golbahar Institute of Higher Education, Golbahar, Iran
[2]Department of Computer Science, University Putra Malaysia, Malaysia

[*]**Corresponding author:** 1. Faezeh Rohani, Department of Computer Science, Sanabad Golbahar Institute of Higher Education, Golbahar, Iran, E-mail: faezeh.rohani@ut.ac.ir
2. Mohammad Amin MoghaddasiFar, Department of Computer Science, Sanabad Golbahar Institute of Higher Education, Golbahar, Iran, E-mail: amin.moghaddasi@alumni.ut.ac.ir

Citation: Mohammad Amin Moghaddasi Far, Faezeh Rohani and E Brhravesh (2015) An Active Algorithm to Gray-scale Digital Image Forgery Detection based on Cellular Automata and LU Decomposition. J Comput Sci Softw Dev 1: 001.

Abstract

A reliable active method for grayscale digital image forgery detection presents in this paper. Our method is based on LU decomposition (Lower Upper Triangular Matrix) of the original JPEG image and one dimensional cellular automata. First we decompose the JPEG input image's matrix and calculate some dominant values of both lower and upper matrixes of the original image, and then we arrange these values into the one dimensional cellular automata. Next, we apply linear cellular automata rules to create a robust cipher key from these values and we embed the cipher key into the spatial domain to authenticate and validate the original image. We applied our algorithm on 100 number of grayscale digital images of size 800 × 800. The experimental results have illustrated the performance and reliability of the proposed algorithm.

Keywords: Digital image forgery detection; Cellular Automata; LU Decomposition.

I. Introduction

The security of digital information (e.g., digital images) has been around for several years now since they are widely used in many areas including medical, industrial, and commercial applications.

These days, it is quite easy to modify the digital content of images while a bunch of powerful tool sets are available [1]. Digital image forgery detection methods are significance in content authentication and validity protection for digital images. The forgery detection techniques that are developed for digital images are mainly classified into active and passive approaches [2 - 6]. While the active methods insert data or signature at the time of digitizing, the passive methods operate in the absence of any data or signature [1 - 3]. In the active methods, we embed data into the original image to protect it against the forgery, where in the passive methods we don't have the original image and we should investigate some features of the image for example on statistical anomalies, correlations, compressions and measurements of objects in the existence image to detect forgery. Passive approaches can be grouped into five categories: pixel-based, format-based, physical-based, camera-based and geometric-based [1].

Active approaches can be divided into two categories by the embedding position spatial domain or frequency domain data [2, 7]. Spatial domain techniques have already developed earlier and are easier to implement but are limited in robustness [5 - 7]. For validation and authentication aspects, the data which is embedded in spatial domain should be unpredictable, invisible and also sensitive to any modification [1, 4, 6]. Data embedding in the spatial domain consists of insertion and detection stages. The insertion algorithms are used to embed the data into the digital image and detection algorithms extract those data.

In this paper we proposed an active method to detect digital image forgery in a reliable manner. We employ LU decomposition and its statistical dominant values and one dimensional cellular automata to create a cipher key. This key has the image features and completely related to digital image that every small change in the content of digital image will change the key value without any exception.

The rest of the paper is arranged as follows. A quick review on the research area is done in section II. We then describe LU decomposition fundamentals in Section III which we employ that in our proposed algorithm. Section IV introduces the concept of one dimensional cellular automaton. Section V illustrates our proposed model by using cellular automata rules. Section VI and VII are the experimental results and conclusion respectively.

II. Related Work

In this section we show the current works and recent advances in the research area. In 2009, Faird [1] provided a nice survey on image forgery detection strategies which was divided into two main categories as active and passive methods.

In 2011, Malakooti et al. [3] developed an active image forgery detection pipeline which utilized one dimensional cellular automaton along with some statistical information as relevant image features. Based on the experiments they have done, the proposed algorithm worked well for both gray-scale and color images.

In 2012, Tafti et al. [6] proposed more robust technique which used a combination of one dimensional cellular automata and SVD to tackle the problem of active image forgery detection. In 2013, Maarefdoust et al. [5] made an image encryption algorithm which might be also useful in the way of image forgery detection.

In 2014, Tafti et al. [2] designed two different active image forgery detection algorithms and they examine their proposed framework using different scenarios.

III. LU Decomposition

In linear algebra, LU decomposition is a matrix decomposition which writes a matrix as the product of a lower triangular matrix and an upper triangular matrix. The product sometimes includes a permutation matrix as well [8].

Let A be a square matrix. An LU decomposition is a decomposition of the form A= LU. Where L and U are lower and upper triangular matrices (of the same size) respectively. This means that L has only zeros above the diagonal and U has only zeros below the diagonal [8] [9]. For a 3 × 3 matrix, this becomes:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{bmatrix}$$

Here we show a small example. Assume that we have a matrix as A:

$$A = \begin{bmatrix} 2 & 7 \\ 5 & 4 \end{bmatrix} = \begin{bmatrix} l_{11} & 0 \\ l_{21} & l_{22} \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} \\ 0 & u_{22} \end{bmatrix}$$

To find the LU decomposition of this simple matrix, we should simply solve the linear equations:

$L_{11} U_{11} + 0 = 2$

$L_{11} U_{12} + 0 = 7$

$L_{21} U_{11} + 0 = 5$

$L_{21} U_{12} + L_{22}U_{22} = 4$

Such a system of equations is underdetermined. In this case any two non-zero elements of L and U matrices are parameters of the solution and can be set arbitrarily to any non-zero value [8, 9]. Therefore to find the unique LU decomposition, it is necessary to put some restriction on L and U matrices. For example, we can require the lower triangular matrix L to be a unit one (e.g., set all the entries of its main diagonal to ones, L_{11}=1 and L_{22}=1). Now, the system of equations has the following solution:

$U_{11} = 2$

$U_{12} = 7$

$L_{21} = 2.5$

$U_{22} = -13.5$

Then, we put these values into the LU decomposition. Therefore:

$$A = \begin{bmatrix} 1 & 0 \\ 2.5 & 1 \end{bmatrix} \begin{bmatrix} 2 & 7 \\ 0 & -13.5 \end{bmatrix}$$

IV. Cellular Automata Basics

The history of cellular automata dates back to the 1940s with Stanislaw Marcin Ulam [10]. This polish mathematician was interested in the evolution of graphic constructions generated by simple rules [10]. The base of his construction was a two-dimensional space divided into "cells", a sort of grid. Each of these cells could have two states: ON or OFF [10]. A cellular automaton is a discrete dynamic model in space and time [10]. All of the cells arrange in the regular form and have a finite number of states. The states are updated with a local rule. Figure 1 shows a simple two state and one dimensional cellular automata with a line of cells. A specific cell can be either be on (value = 1) or off (value = 0). The closest cells to cell X are those to its immediate right and left. In this figure, we have a local neighborhood of three cells. The state of X at the time *t + 1* will be determined by the states of the cells within its neighborhood at the time *t* [10].

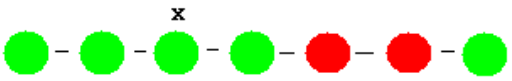

Figure 1. **One dimensional cellular automata with three neighborhoods for cell X.**

We can set a local rule for each cellular automata. For example, we can estimate the value of cell X in time *t+1* with the following rule [10, 11]:

$Cell[X]_{t+1} = Cell[X-1]_t + Cell[X+1]_t$

Assume that the input sequence is 01100 and we want to use the above rule for our cellular automata, then the output sequence will be 11110. Table 1 shows the output of these cellular automata.

Table 1: **An Example of Cellular Automata.**

Cell Number	0	1	2	3	4
Input Sequence (time *t*)	0	1	1	0	0
Cellular Automata Rule	$Cell[X]_{t+1} = Cell[X-1]_t + Cell[X+1]_t$				
Output Sequence (time *t+1*)	1	1	1	1	0

V. Proposed Algorithm

The main idea of our proposed algorithm is to protect a digital image against forgery through creating and embedding a robust cipher key into the spatial domain of an image. We embed the bit sequence of the key into the LSB of the particular pixels in the original image.

Our proposed algorithm performs on a grayscale JPEG image and generates a lossless PNG image with the grayscale mode. We don't generate lossy compression format.

The embedding process based on the cellular automata with XOR local rule (Table 2). Cellular automata have been implemented to create the required cipher key bit sequence. We only use three numbers of statistical information of the LU decomposition matrices of the original image to generate the cipher key. This information consists of arithmetic mean, median, and the statistics range as well as the dominant singular values of the image. If anybody wants to modify a digital image, then the statistical information of these particular matrices, we mean L and U matrices will be changed and the output of the proposed cellular automata will be damaged.

Table 2: Proposed Cellular Automata with X or Local Rule (Implemented For Six Cells).

Cell Number	Input Value (time *t*)	Rule
0	Mean of the all values in the L Matrix from LU decomposition of the original image.	$Cell[X]_{t+1} = Cell[X-1]_t$ XOR $Cell[X+1]_t$
1	Mean of the all values in the U Matrix from LU decomposition of the original image.	
2	Median of the values in the L Matrix from LU decomposition of the original image.	
3	Median of the values in the U Matrix from LU decomposition of the original image.	
4	Range of the values in the L Matrix from LU decomposition of the original image.	
5	Range of the values in the U Matrix from LU decomposition of the original image.	

A. Arithmetic Mean

Mean is a method to derive the central tendency of a sample space. If we have sample space {a[1], a[2],… a[n]}, then arithmetic mean is defined via the following equation [9] :

$$mean = \frac{1}{n}\sum_{i=1}^{n} ai$$

B. Median

Median is described as the numeric value separating the higher half of a sample, a population, or a probability distribution, from the lower half [9].

C. Range

It is the difference between the highest and the lowest values in a data set [9].

All of these statistical information is easy to calculate and also exclusive in a data set. Figure 2 shows the block diagram of the proposed method and Figure 3 illustrates the diagram of the proposed cellular automata to create a cipher key base on statistical information of the L and U matrices.

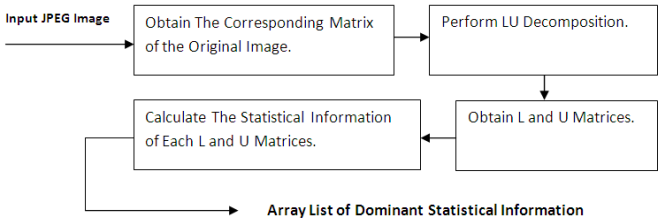

Figure 2: Block Diagram of our Proposed Method.

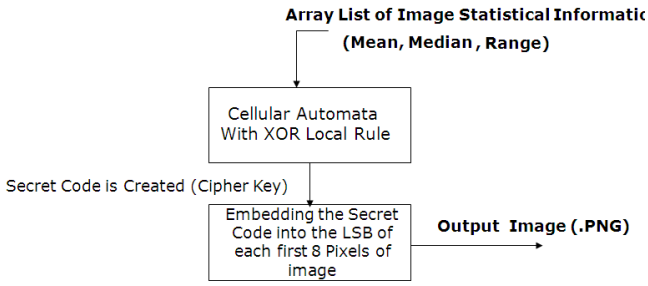

Figure 3: **Block Diagram of our Proposed Cellular Automata to Create a Chipher Key.**

The embedding algorithm in a spatial domain of the original image will be as follows:

A. Data Embedding Algorithm

Input: .JPEG grayscale image to apply data embedding to it for forgery detection.

Output: .PNG grayscale image file.

Step1: Open the JPEG original image and make a corresponding matrix of that.

Step2: Perform the LU decomposition and obtain L and U matrices.

Step3: Calculate the statistical information for each L and U matrices separately and create the array list of these values.

Step4: Perform the cellular automata rule according to the Table 2. This rule performs on the array list to create a cipher key.

Step5: Convert the cipher keys to the binary representation.

Step6: Select the first eight pixels in the original image and embed the binary sequences of cipher key into the LSB of these eight pixels.

The forgery detection algorithm will be as follows:

B. Forgery Detection Algorithm

Input: .PNG image that contains the cipher key.

Output: Digital image forgery detection ALARM.

Step1: Open the .PNG input image and make corresponding digital image matrix.

Step2: initial integer variable *Cipher Value* to zero.

Step3: initial integer variable *Pixel Array Value* to zero.

Step4: Perform the LU decomposition and obtain L and U matrices.

Step5: Calculate the statistical information for each L and U matrices separately and create the array list of these values.

Step6: Perform the cellular automata rule according to the Table 2. This rule performs on the array list to create a cipher key for each partition.

Step7: Select the first eight pixels of the image and extract the LSB binary value of pixels.

Step8: set *Cipher Value* = value of the cipher key that generated in Step 6.

Step9: set *Pixel Array Value* = the extraction value in Step 7.

Step10: If *Pixel Array Value* = = *Cipher Value* then print message "*False Forgery Alarm*"

Else Print message "*True Forgery Alarm*";

The proposed algorithm has been implemented by Java2SE8 and MATLAB R2013, which have the enough strength to embed data into the spatial domain of .JPEG image and also extract data from the .PNG image.

VI. Experimental Results

To prove the performance of the proposed forgery detection method, five experiments will be presented in this section to show the implementation and the results of our proposed system. These are as follow:

- Performance
- True and False Alert
- Diffusion
- Confusion
- PSNR

In order to evaluate the above aspects of our proposed method, we perform several tests on a sample dataset. Our sample dataset contains 100 numbers of grayscale JPEG images (size 800 × 800).

• Performance

We have generated a PNG image as the output of our method with lossless compression. The experiment used a JPEG image of size 800 × 600. Figs 5 to 8 show the original images and data embedded output PNG images which generated via our method to prove the performance of our method.

• True and False Alert

In Table 3, you can see the percentage of true and false detection of digital image forgery which are performed by the proposed method.

Table 3: **True and False Detection of our Proposed Method.**

True Alert (%)	False Alert (%)
91	9

• Diffusion

Diffusion describes the spread of particles through random motion from regions of higher concentration to regions of lower concentration. The time dependence of the statistical distribution in space is given by the diffusion equation. The concept of diffusion is tied to that of mass transfer driven by a concentration gradient, but diffusion can still occur when there is no concentration gradient (but there will be no net flux) (Figure 4) [12].

In cryptography, confusion and diffusion are two properties of the operation of a secure cipher which were identified by Claude Shannon in his paper Communication Theory of Secrecy Systems, published in 1949 [12].

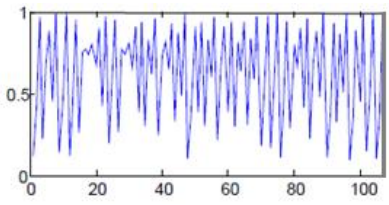

Figure 4: Diffusion for the Secret Key Which is Generated by the Proposed Cellular Automata.

- **Confusion**

It is the lack of clearness or distinctness. One aim of confusion is to make it very hard to find the key even if one has a large number of plaintext-cipher text pairs produced with the same key [12]. Table 4 shows the rate of confusion for our proposed model.

Table 4: **Rate of Confusion for our Proposed Model**. (The Yellow color indicates changing in corresponding values.)

Mean	Median	Range	
42.5	35	90	Original Image
40	32	90	10 Pixel Altered
39.2	31	88	30 Pixel Altered

- **PSNR**

Measuring the PSNR (peak signal-to-noise ratio) of our proposed method is the next experiment. It indicates the maximum possible power of a signal and the power of corrupting noise that affects the output. We mentioned that all pixels in both of the input and output images in our proposed method are based on 8 bits. We implement PSNR function in MATLAB R2009a. When we run this function in MATLAB R2009a, it indicates that the PSNR for our proposed algorithm was 34.81. Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, where higher is better [13]. Therefore, our proposed algorithm has a good PSNR.

VII. Conclusion

Our proposed approach has been applied successfully for digital image forgery detection. In this paper we present a new method based on LU decomposition and cellular automata which was done by calculating the invaluable statistical information of the LU decomposition matrices mean and median and range. The cellular automata rule also generates a robust cipher key which can be used to embed into the image. Our method needs the original image to forgery detection (Figures 5 - 8) [14, 15].

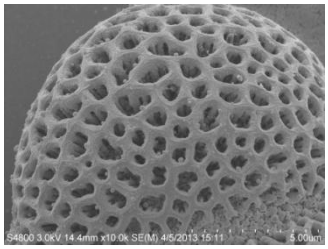

Figure 5: Original Image [14, 15].

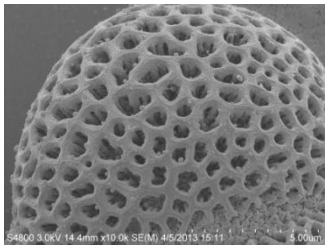

Figure 6: Data Embedded Image based on Cellular Automata.

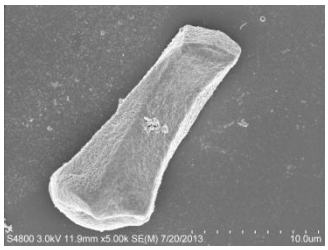

Figure 7: Original Image [14, 15].

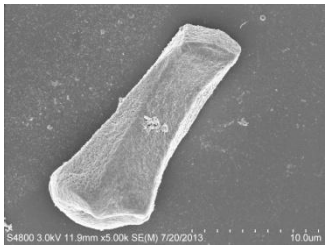

Figure 8: Data Embedded Image based on Cellular Automata.

The experimental results obtained from this method, specially the confusion, diffusion and true and false alert of our proposed model, clearly shown the performance and reliability of our system. As a part of our future work, we would examine and compare our proposed system with other similar frameworks in the research area. In future, this research can also use as a practical biomedical imaging method [16, 17].

VIII. References

1. Farid Hany (2009) "Image forgery detection." Signal Processing Magazine, IEEE 26, no. 2: 16-25.
2. Tafti Ahmad Pahlavan, Hamid Hassannia (2014) "Active Image Forgery Detection Using Cellular Automata." In Cellular Automata in Image Processing and Geometry, pp. 127-145. Springer International Publishing.
3. Malakooti MV, M Ashourian, S Janosepah (2011) "Digital image forgery detection through data embedding in spatial domain and cellular automata." In Digital Content, Multimedia Technology and its Applications (IDCTA), 7th International Conference, pp. 11-15. IEEE.
4. Tafti Ahmad Pahlavan, Safoura Janosepah (2011) "Digital images encryption in frequency domain based on DCT and one dimensional cellular automata." In Informatics Engineering and Information Science, pp. 421-427. Springer Berlin Heidelberg.
5. Tafti Ahmad Pahlavan, Reyhaneh Maarefdoust (2013) "Digital Images Encryption in Spatial Domain Based on Singular Value Decomposition and Cellular Automata." International Journal of Computer Science and Information Security 11: 121-125.
6. Malakooti MV, Ahmad Pahlavan Tafti, Faezeh Rohani, Mohammad Amin Moghaddasifar (2012) "RGB digital image forgery detection using Singular Value Decomposition and One Dimensional Cellular Automata." In Computing Technology and Information Management (ICCM), 8th International Conference, vol. 1, pp. 483-488. IEEE.
7. Mohan B Chandra, S Srinivas Kumar (2008) "A robust image watermarking scheme using singular value decomposition." Journal of Multimedia 3: 7-15.
8. Golub Gene H, Charles F Van Loan (2012) Matrix computations. Vol. 3. JHU Press.
9. Grimaldi Ralph P (2006) Discrete and Combinatorial Mathematics, 5/e. Pearson Education India.
10. Wolfram Stephen (1986) Theory and applications of cellular automata. Vol. 1. Singapore: World Scientific.
11. Urias Jesus (2000) "Cryptography primitives based on a cellular automaton." In Coding Theory, Cryptography and Related Areas, pp. 244-248. Springer Berlin Heidelberg.
12. Trappe Wade, Lawrence C Washington (2006) Introduction to cryptography with coding theory. Pearson Education India.
13. Welstead Stephen T (1999) Fractal and wavelet image compression techniques. (Bellingham, WA: SPIE Optical Engineering Press.
14. Tafti A Pahlavan, AB Kirkpatrick, HA Owen, Z Yu (2014) "3D Microscopy Vision Using Multiple View Geometry and Differential Evolutionary Approaches." In Advances in Visual Computing, pp. 141-152. Springer International Publishing.
15. Tafti Ahmad P, Andrew B Kirkpatrick, Zahrasadat Alavi, Heather A Owen, Zeyun Yu (2015) "Recent advances in 3D SEM surface reconstruction." Micron 78: 54-66.
16. Rohani Faezeh, Hamid Hassannia, Mohammad Amin MoghaddasiFar, Elham Sagheb (2014) "Human cell detection in microscopic images through discrete cosine transform and Gaussian mixture model". Computational Biology and Bioinformatics 2: 52-56.
17. Rohani Faezeh, Mohammad Amin Moghaddasi Far, Fatemeh Fazayeli Bavojdan (2015) "From Business Process Management to Flexible Image Analysis Applications: A Case Study." Computational Biology and Bioinformatics 3: 40-44.