Optics Communications xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

A novel cellular automata based technique for visual multimedia content encryption

Savvas A. Chatzichristofis [a,*], Dimitris A. Mitzias [a], Georgios Ch. Sirakoulis [a], Yiannis S. Boutalis [a,b]

[a] Department of Electrical & Computer Engineering, Democritus University of Thrace, 67100, Xanthi, Greece
[b] Department of Electrical, Electronic and Communication Engineering, Chair of Automatic Control, Friedrich-Alexander University of Erlangen-Nuremberg, 91058 Erlangen, Germany

ARTICLE INFO

Article history:
Received 24 November 2009
Received in revised form 7 May 2010
Accepted 14 June 2010
Available online xxxx

Keywords:
Cellular automata
Image encryption
Lossless encryption
Coordinate logic filters

ABSTRACT

This paper proposes a new method for visual multimedia content encryption using Cellular Automata (CA). The encryption scheme is based on the application of an attribute of the CLF XOR filter, according to which the original content of a cellular neighborhood can be reconstructed following a predetermined number of repeated applications of the filter.
The encryption is achieved using a key image of the same dimensions as the image being encrypted. This technique is accompanied by the one-time pad (OTP) encryption method, rendering the proposed method reasonably powerful, given the very large number of resultant potential security keys. The method presented here makes encryption possible in cases where there is more than one image with the use of just one key image. A further significant characteristic of the proposed method is that it demonstrates how techniques from the field of image retrieval can be used in the field of image encryption. The proposed method is further strengthened by the fact that the resulting encrypted image for a given key image is different each time. The encryption result depends on the structure of an artificial image produced by the superposition of four 1-D CA time–space diagrams as well as from a CA random number generator.
A semi-blind source separation algorithm is used to decrypt the encrypted image. The result of the decryption is a lossless representation of the encrypted image. Simulation results demonstrate the effectiveness of the proposed encryption method. The proposed method is implemented in C# and is available online through the img(Rummager) application.

1. Introduction

In recent years, the rapid spread of the internet, as well as the proliferation of visual multimedia recording devices has created an exigency calling for an effective image encryption method. Whereas in the past, encryption was by and large the concern of military applications, nowadays it is becoming necessary in more and more sectors. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms are not suitable for practical image encryption [1].

Modern bibliographies include numerous image encryption algorithms. These algorithms can be classified according to their ability to render the decrypted image as a precise facsimile of the encrypted image (lossless encryption), and according to the method used to achieve the encryption. The most common encryption methods are divided into 4 categories: Those algorithms using SCAN-Based [2,3] techniques, algorithms using Chaos-Based [4–6] techniques, algorithms using Structure-Based [7] techniques, and finally those algorithms where the encryption techniques combine elements from the other techniques or use elements borrowed from other scientific disciplines. However, each of them has its strengths and weaknesses in terms of security level, speed, and resulting stream size metrics [3].

This paper proposes a new encryption method for visual multimedia which could preliminarily be classified under the lossless encryption category. The proposed algorithm is modeled using cellular automata (CA) and comprises a semi-blind source separation algorithm which adopts the features of a one-time cipher (OTP) encryption, given that the encryption key is an image of the same dimensions as the image being encrypted. This aspect renders the encryption method secure enough [8].

CAs, first introduced by von Neumann [9], are models of physical systems, where space and time are discrete, and interactions are local. CA are very effective in simulating physical systems and solving scientific problems, because they can capture the essential features of systems where global behavior arises from the collective effect of simple components which interact locally [10,11]. Nontrivial CA are obtained whenever the dependence from the values of each site is nonlinear [12]. As a result, any physical system satisfying differential equations may be approximated by a CA, by introducing finite differences and discrete variables [13–19]. On the other hand, CAs are one of the computational structures best suited for a VLSI realization [20–23]. Hardware implementation of CA is described in details in [24,25]. The CA architecture offers a number of advantages and beneficial features such as simplicity, regularity, ease of mask generation, silicon-area utilization, and locality of interconnections

* Corresponding author.
E-mail address: schatzic@ee.duth.gr (S.A. Chatzichristofis).

0030-4018/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2010.06.043

[14,21]. Two-dimensional CA have been used extensively for image processing and pattern recognition [26,27].

Regarding image encryption, some works based on CA are already reported in literature. In [28], CA were used to produce the bit stream of the key in a Vernam cipher cryptography. In [29] a family of basis functions, generated from the evolving states of CA, is used to compress and encrypt data. In [3], an image encryption method is based on permutation of the pixels of the image and replacement of the pixel values. The permutation is done by scan patterns that were generated by the SCAN methodology. The pixel values are replaced using a progressive CA substitution with a sequence of CA data that is generated from the CA evolution rules. CAs were also proposed for public-key cryptosystems by Guan [30] and Kari [31]. In such systems two keys are required: one key is used for encryption and the other for decryption.

In [32] an image security system based on the replacement of the pixel values using recursive cellular automata is presented. This method is lossless and can be classified as a symmetric private key encryption method. Finally, cellular automata have been utilized in the literature for image encryption in [30,31].

The algorithm proposed in this paper is based on an attribute of the exclusive-OR (XOR) logic gate, according to which its application to a CA of $N\times N$ dimensions has the ability to reconstruct the CA after $\frac{N}{2}$ repetitions. The process is analyzed in Section 2. The proposed method uses an additional key for fast decryption of the encrypted image. This key is a Compact XML file which gives the capacity in the proposed method, using the same key image, to produce a different encryption result each time where it is applied in an image. This feature is not present in other CA encryption methods. The production process of this key is described in Section 3. Section 4 describes the process of application of the XOR gate attribute to the decryption of both the key image and the secret image, as well as the method of merging these two images. Section 5 describes the proposed image decryption process. Section 6 develops the encryption characteristics and checks for security issues regarding the application of the proposed method. Finally, the conclusions are drawn in Section 7.

2. Application of the CLF-XOR filter on CA

The implementation of the XOR gate in the CA is quite widespread in the literature, as well as the recursiveness of the resulting outcomes [33]. In the proposed method, since the content of CA derived from images, the implementation of the XORgate is considered as a Coordinate Logic Filter-XOR (CLF-XOR) [34]. CLFs are logic operations (AND, OR, NOT, XOR and their combinations) among the corresponding binary values of two or more signals or image pixels. They are actually nonlinear digital filters that are based on the execution of Coordinate Logic Operations among the pixels of the image. CL filters can execute the morphological operations (erosion, dilation, opening and closing) and the successive filtering and managing of the residues. Therefore CL filters are suitable to perform the range of tasks and applications that are executed by morphological filters, achieving similar functionality [35]. This paper presents an attribute of the CLF-XOR when applied to a 2-D CA of $N\times N, N=2^p, p\in Z$ dimensions. The CA is comprised of a linear two-dimensional (2-D) table of identical cells each of which can be found in k states. The local state of cell x,y during time step t is given by the formula:

$$s_t^{x,y}\in\sum = \{0,1,\ldots,k-1\} \tag{1}$$

The total state of a cell, i.e. s_t, during time t is the configuration of the whole table:

$$st = \left(s_t^{0,0},\ s_t^{0,1}, s_t^{0,2},\ \ldots,\ s_t^{N-1,N-1}\right)\in\sum^{N\times N} \tag{2}$$

where N is the size of the square 2-D-CA. At every time step all the cells of the CA recalculate their state concurrently according to the following rule:

The values of the cells in the Moore [36] neighborhood with radius $r=1$, participate in the logical operation XOR and their result is placed in the central cell of the neighborhood.

$$S_1^{x,y} = S_0^{x-1,y-1}\oplus S_0^{x,y-1}\oplus S_0^{x+1,y-1}\oplus S_0^{x-1,y}\oplus \oplus S_0^{x,y}\oplus S_0^{x+1,y}\oplus S_0^{x-1,y+1}\oplus S_0^{x,y+1}\oplus S_0^{x+1,y+1}. \tag{3}$$

The application with CLF-XOR produces a TRUE output if an odd number of inputs in the neighborhood are TRUE.

Boundaries of the CA are periodical and displayed in Fig. 1.

This can be visualized as taping the left and right edges of the rectangle to form a tube, then taping the top and bottom edges of the tube to form a torus (doughnut shape). Application of the rule for $t=\frac{N}{2}$ times demonstrates the attribute returning the CA to state s_0 (initial state).

$$\begin{aligned} S_1^{x,y} &= S_0^{x-1,y-1}\oplus S_0^{x,y-1}\oplus S_0^{x+1,y-1}\oplus S_0^{x-1,y}\oplus \\ &S_0^{x,y}\oplus S_0^{x+1,y}\oplus S_0^{x-1,y+1}\oplus S_0^{x,y+1}\oplus S_0^{x+1,y+1} \\ S_2^{x,y} &= S_1^{x-1,y-1}\oplus S_1^{x,y-1}\oplus S_1^{x+1,y-1}\oplus S_1^{x-1,y}\oplus \\ &S_1^{x,y}\oplus S_1^{x+1,y}\oplus S_1^{x-1,y+1}\oplus S_1^{x,y+1}\oplus S_1^{x+1,y+1}. \\ &\ldots \\ S_{\frac{N}{2}}^{x,y} &= S_0^{x,y} \end{aligned} \tag{4}$$

Additionally, the repetition of the rule per $t=\frac{N}{2}$, repeats the same result, confirming the periodicity of the attribute. Application of a CLF-XOR filter to a 2-D-CA of 2×2 and 4×4 dimensions is presented in Fig. 2. It should be noted that if the CA boundaries are fixed, $2\times N$ time steps are required for periodicity to be observed. If an image of the same dimensions is considered to be a CA, the attribute is repeated. In the case of a color image, the process is applied independently to each individual channel. In order to illustrate the CLF-XOR application on images we give the following:

Let us consider an image j with size $N\times N$. Given that this is a color image, it consists of 3 layers. One layer for RED $L(j)_R$, one layer for GREEN $L(j)_G$, and one layer for BLUE $L(j)_B$. Each layer comprises of $N\times N$ 8 bit numbers. Each pixel $j_{x,y}$ of image j requires 24 bit for its display and has the value $(L(j_{x,y})_R, L(j_{x,y})_G, L(j_{x,y})_B)$.

During the filter application, each layer is processed individually. More specifically, each layer is considered as a 2-D CA 256-state, that is, the cell values are integers in [0,255] which are subsequently converted in binary form. The CLF-XOR filter is applied on every state of the CA. Essentially, this filter executes XOR operation between the

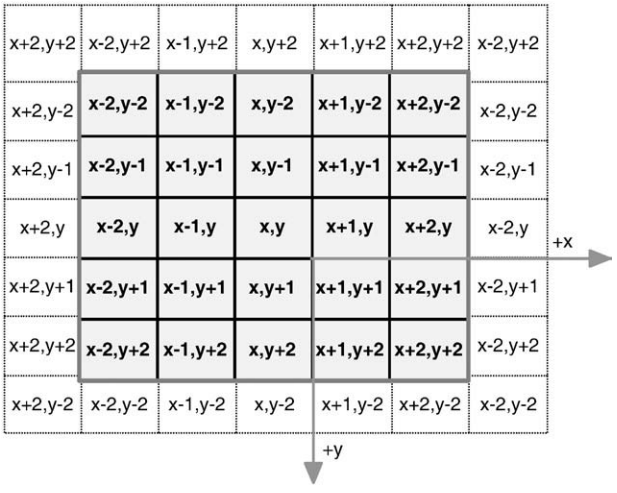

Fig. 1. Boundaries of the CA.

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

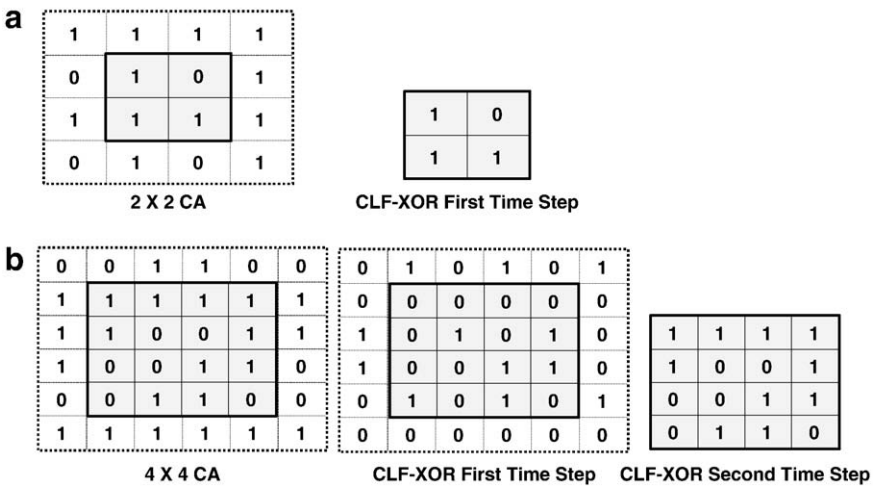

Fig. 2. (a) Application of CLF-XOR to a 2-D CA size of 2×2 and (b) Application of CLF-XOR to a 2-D CA size of 4×4.

binary form values of the 9 cells that belong to the neighborhood on which the filter is applied. The application of the CLF-XOR filter on nine (9) 8-bit values results in an 8-bit number. The operation outcome is placed in the central cell of the neighborhood. This procedure is repeated for all the pixels/cells of every layer, while special attention must be paid for the boundary pixels/cells (which are regarded as periodical).

The same procedure must be followed when the filter is applied more than one times, with new values being generated for all the CA cells upon every iteration completion. The next iteration of the filter application is performed on these new CA values.

As already mentioned the same procedure is followed for all the layers. The resultant 3 layers are combined in order to form the full distorted image. Each pixel of this image takes the value $(L(j_{x,y})_R, L(j_{x,y})_G, L(j_{x,y})_B)$ with $x,y \in [0, N-1]$.

It is worth noting that during the interim time marks, the image is greatly distorted, making it impossible to be recognized. The whole procedure is depicted in Fig. 3.

3. Compact XML KEY

As previously mentioned, the proposed method uses 2 keys for the encryption method. The first key is an image with the same dimensions as the image to be encrypted, and the second key is a Compact XML KEY. XML (Extensible Markup Language) is a general-purpose specification for creating custom markup languages.

The Compact XML KEY is generated on the sender site and is directly connected with the basic key of the encryption process, hereafter referred to as the KEY image. The Compact XML KEY includes $\frac{N}{2}-2$ entries where N is the dimension of the square image to be encrypted, hereafter referred to as DATA image. Each file entry includes four (4) fields. One field contains an image descriptor, while the rest 3 fields contain a set of CA based random integer numbers.

The Compact XML KEY generation procedure is illustrated in Fig. 5 and analyzed as follows:

In order to send the DATA image, the parameters R_1, R_2, C_1 and C_2 must be first selected by the user. Their values are integer numbers in $\{0, N\}$. These parameters correspond to the 2 rows and 2 columns of the KEY image, respectively. The selection of these values can be done by any means, however the random number generator presented later in this section is suggested.

The CLF-XOR described in Section 2 is applied to the KEY image, $\frac{N}{2}-2$ times. An important note is that at each iteration of the filter application, the filter is applied on all the 3 layers of the KEY image. The resultant image after each application of the CL filter is defined as the KEϒimage$_p$, $p \in \left\{1, \frac{N}{2}\right\}$. The rows and columns R_1, R_2, C_1 and C_2 are taken from each KEϒimage$_p$ and used to construct an artificial image AI_p. The artificial image will be used for the extraction of the descriptors included in the XML KEY.

In order to proceed with the formation of the AI_p, the aforementioned image is considered to be the original configuration of a CA model with its cells taking discrete values from {0,…,255}. However, instead of profound considering 2-D CA, each row and column of the 4 parameters that correspond to the aforementioned image as shown in Fig. 4 is considered to be a 1-D N-size CA. Consequently four different CAs each one initial configuration corresponding to the aforementioned row or column, respectively, are synchronously evolved for $\frac{N}{2}$ time steps and result in the corresponding time–space CA diagram. The boundary conditions of the CA are set equal to zero (Fig. 4). The CA rule which is the same for all the 1-D CA taken under consideration is described below as a pseudocode:

```
for t = 1 : N/2
 for i = 1 : N                    /* N is the dimension of the 1-D CA
   if (t − i) = 0 or
      (t + i) = (N + 1)           /* our main interest is focused on
                                     the boundary CA cells
     S_t^i = 0;                   /* the local CA cell state returns to
                                     zero
   else
     S_t^i = S_t^i                /* the CA cell state remains unchanged
   end
 end
end
```

The final artificial image AI_p ready for the next step of our algorithm is produced by the superposition of each of the four (4) 1-D CA time–space diagrams as illustrated in Fig. 4(c). The whole procedure is depicted in Fig. 4.

The extraction of a descriptor is requested from each AI_p in order to describe this image as uniquely as possible. Due to the artificial construction of these images, the use of classic color or texture descriptors result in similar vectors for each AI_p. For this reason, a compact composite descriptor (CCD) has been selected, as it combines color and texture characteristics in a vector. A compact version of

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

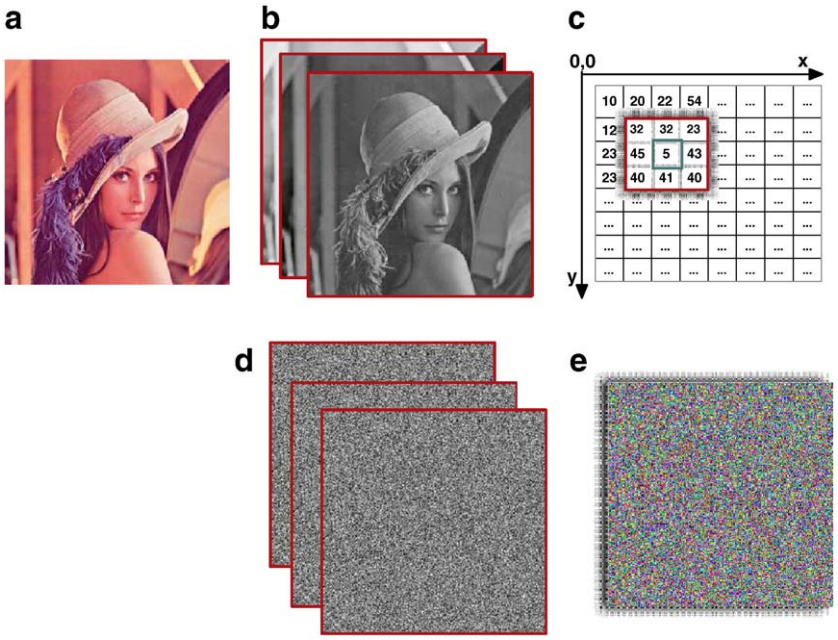

Fig. 3. (a) Original Image, (b) The three (3) image layers, one layer for the RED channel, one layer for the GREEN channel, and one layer for the BLUE channel, (c) An example neighborhood on which the CLF-XOR is applied — The cell values are converted to binary form and participate in the XOR operation. The result replaces the central cell of the neighborhood, (d) The three (3) image layers after the CLF-XOR application and (e) The distorted image. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

the color and edge directivity descriptor (CEDD) proposed in [37] eb1 is extracted from each AI_p. The CEDD descriptor incorporates both color and texture features in a histogram while it is limited to 54 bytes per image.

For the CEDD generation, the image is initially split in a preselected number of blocks. For each block a color histogram is computed over the HSV (Hue, Saturation and Value) color space using a fuzzy linking system. Several fuzzy based rules are applied to obtain a 24-bins histogram for every block. Each histogram bin represents a different color from a preset palette.

For every block texture information extraction, the 5 filters suggested from MPEG-7 Edge Histogram Descriptor are employed. These filters are used to export the texture information related to the edges presented in the image, and are classified in vertical, horizontal, 45-degree diagonal, 135-degree diagonal and non-directional edges. Finally, utilizing an early fusion method described in detail in [37,38] results a histogram with 144 bins ahd storage requirements smaller than 54 bytes per image. This paper replaces the 24-bins histogram used by the CEDD, with a 10-bins histogram as proposed in [39]. Thus the descriptor size is limited to 23 bytes per image. Experiments using Wang's image database [40] for random values R_1, R_2, C_1 and C_2 have shown that the Compact CEDD descriptor can give a unique description for each AI_p.

The descriptor value for each AI_p is registered in an XML file. In addition, for each Artificial Image AI_p, 18 random numbers are also registered: three numbers for the $X-KEY_1[D]$, $D \in [0,2]$, three numbers for the $X-KEY_2[D]$, $Din[0,2]$, and twelve numbers for the $X-KEY_3[D,Z]$, $D \in [0,2]$, and $Z \in [0,3]$.

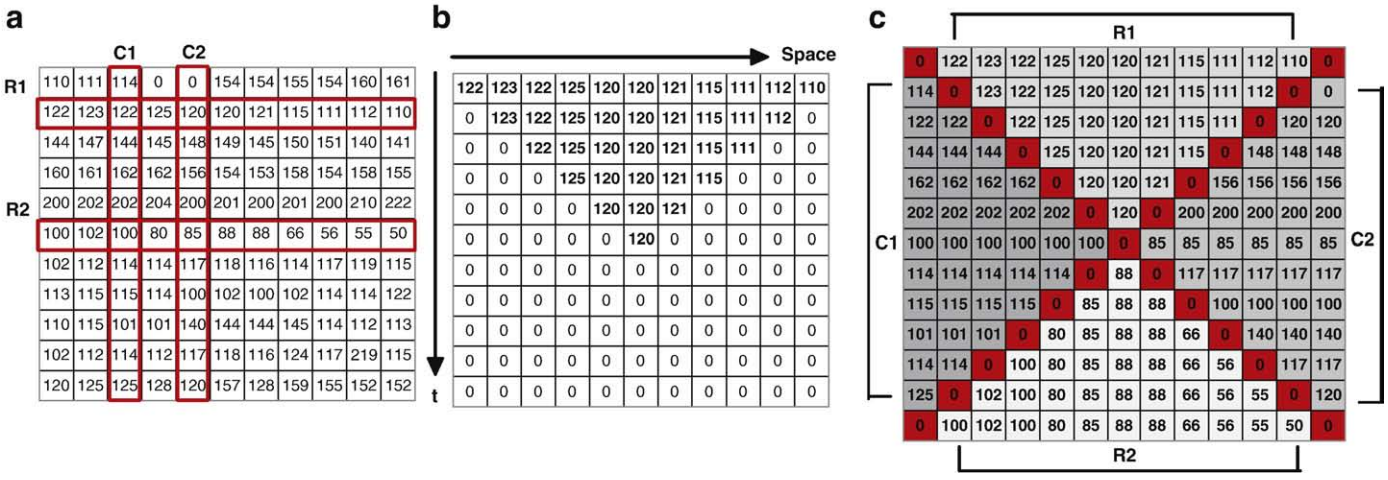

Fig. 4. (a) The original KEYimage$_p$ and the four (4) initial parameters C_1 ,C_2 ,R_1 and R_2, (b) evolution of one of the four 1-D CA, namely the selected R_1 one, for $\frac{N}{2}$ time steps, and (c) the superposition of the four resulted time–space diagrams that comprise the final image. The four (4) resulted time–space diagrams are combined clockwise with the order R_1, C_2, R_2 and C_1.

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

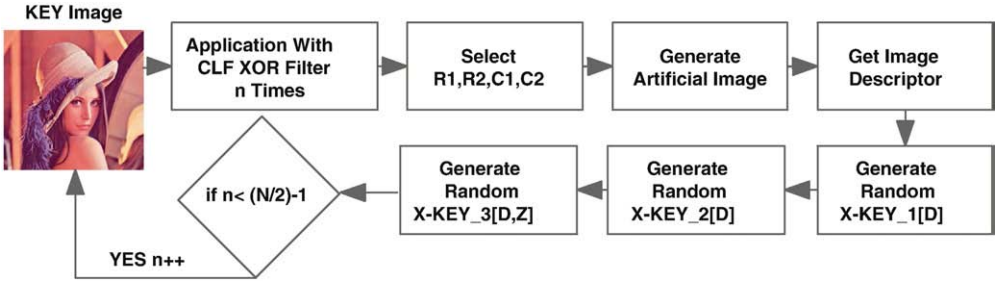

Fig. 5. Process of compact XML KEY generation.

The $X-KEY_1[D]$ and $X-KEY_2[D]$ value range is $\left\{1,\frac{N}{2}-1\right\}$ while the $X-KEY_3[D,Z]$ value breadth is $\left\{1,\frac{N}{4}-1\right\}$. The use of these values is described in Section 4 and Section 5.

Special concern is taken in order to avoid the appearance of the same values for the $X-KEY_1[D]$ and $X-KEY_2[D]$. In addition, during the generation of the numbers concern is taken in order not to include three times the same value in the triad of numbers that configure the $X-KEY_1[D]$ and $X-KEY_2[D]$. That is, the equalities $X-KEY_1[0]=X-KEY_1[1]=X-KEY_1[2]$ and $X-KEY_2[0]=X-KEY_2[1]=X-KEY_2[2]$ should never hold.

In order to generate these numbers, a one-dimensional (1-d) Cellular Automaton (CA) for pseudorandom number generation (PRNG) [41] is used. This generator is based on the real time clock sequence (analytical time description) and can generate high-quality random numbers which can pass all of the statistical tests of DIEHARD as well as NIST [42], which seems to be the most powerfully complete general test suites for randomness. In order to accomplish the aforementioned requirements so as to generate high-quality random numbers, a random sequence which originates from the real time computer clock sequence was used. More specifically, in order to find out the initial CA state configuration and the total number of CA cells the product of all the above numbers, namely day, month, year, hour, min and seconds was calculated. The result of this operation produced a binary number which indicated the initial CA configuration and simultaneously the length of the CA. More details regarding the usage of the aforementioned CA PRNG can be found on [41].

The entire Compact XML KEY generation procedure is illustrated in Fig. 5.

4. Visual multimedia content encryption

The proposed encryption method is described as follows: Users of both the receiver site and the sender site know the KEY image. At the sender site the user selects the values R_1,R_2,C_1 and C_2, and using the method described in Section 3, he/she constructs the Compact XML KEY. If more than one image is to be sent during the communication session, this process is only undertaken the first time. The Compact XML Key is also sent to the receiver site. The procedure of exchanging both the KEY image and the Compact XML KEY is not a feature of the proposed method and is not described.

One of the merits of the proposed method is that, although it relates to classic OTP encryption, it is able to overcome the weakness of being able to send only one image for each key.

The perfect security of the OTP relies crucially on the encryption of a single image. To see this, suppose images M_1 and M_2 are encrypted using the KEY image K. The adversary obtains $C_1=K\oplus M_1$ and $C_2=K\oplus M_2$. XOR-ing them together, it obtains $M_1\oplus M_2$. This however provides partial information about the data and in particular, if the adversary would now happen to learn M_1, it would deduce M_2, which is not desirable.

In the proposed method, because of the application of the CLF-XOR in the KEY image, the image that is finally used to encrypt the DATA Image is different. For each KEY image there are $\frac{N}{2}-1$ ($N=$ the dimension of the images) different KEY images. Given that each time a different number of repetitions of CLF XOR applied to the KEY image shall be used, the proposed method can encrypt $\left(\frac{N}{2}-1\right)$ images.

For each DATA image to be sent, a value $l\in\left\{1,\frac{N}{2}-1\right\}$ is selected using a random number generator referred in Section 3. If more than one image is to be encrypted with the same KEY Image a test is always done to see if the l has not been used before.

The CLF-XOR filter is applied to the KEY image, l times. Next, utilizing the same values $R_1,R_2,C_1,C_2\in\{0,N-1\}$, used to generate the Compact XML KEY, the sender site user selects the appropriate rows and columns from the l times filtered KEY image and generates the AI_l.

The descriptor is extracted from the AI_l image and its distance from descriptors contained in the Compact XML KEY is calculated. The distance between descriptors is measured using the Tanimoto coefficient, as recommended in [38]. The effectiveness of the Tanimoto coefficient is proven in [43–45].

$$D(i,j)=T_{ij}=t\left(x_i,x_j\right)=\frac{x_i^Tx_j}{x_i^Tx_i+x_j^Tx_j-x_i^Tx_j} \tag{5}$$

where x^T is the transpose vector of the descriptor x.

In the absolute congruence of the vectors, the Tanimoto coefficient takes the value 1, while in the maximum deviation the coefficient tends to zero.

The values $X-KEY_1[D]$, $X-KEY_2[D]$ and $X-KEY_3[D,Z]$ are read from the XML entry in which the distance of the 2 descriptors is equal to 0.

Next, the CLF-XOR filter is applied once again $X-KEY_1[0]$ times to the Red channel, $X-KEY_1[1]$ times to the Green channel and $X-KEY_1[2]$ times to the Blue channel of the KEY image. Also, the CLF-XOR filter is applied $X-KEY_2[0]$ times to the Red channel, $X-KEY_2[1]$ times to the Green channel and $X-KEY_2[2]$ times to the Blue channel of the DATA image.

The 2 generated images are merged as follows:The filtered KEY image is defined as KI_{X-KEY_1}, the filtered DATA image as DI_{X-KEY_2} and the ENCRYPTED' image as EI.The merging process of each color channel of the 2 images is described by the following formula (MOD 256):

$$\begin{aligned}&EI[x,y]=KI_{X-KEY_1}[x,y]+DI_{X-KEY_2}[x,y]\\&x,y\in\{0,N-1\}\\&EI[x,y],KI_{X-KEY_1}[x,y],DI_{X-KEY_2}[x,y]\in\{0,\ldots,255\}\\&if\,(EI[x,y]\notin\{0,255\})EI[x,y]=EI[x,y]-255\cdot\end{aligned} \tag{6}$$

Finally, the ENCRYPTED' image is separated in $Z\in[0,3]$ non-overlapped square blocks. The CLF-XOR filter is applied $X-KEY_3[0,Z]$ times to the red channel, $X-KEY_3[1,Z]$ times to the green channel and $X-KEY_3[2,Z]$ times to the blue channel of the Z block of the ENCRYPTED' image. The procedure is repeated for all the Z blocks

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

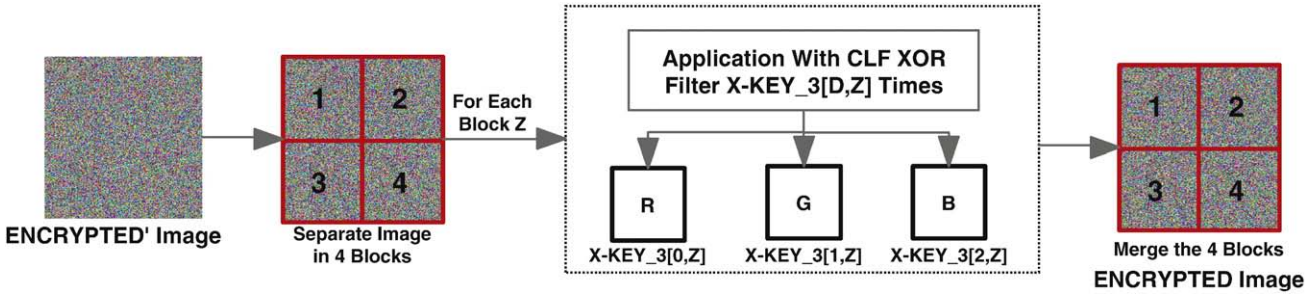

Fig. 6. Block filtering.

and illustrated in Fig. 6. The final ENCRYPTED Image is the combination of the four filtered blocks.

The dimensions of the final image to be sent will be $(N+2)\times(N+2)$. The rows and columns R_1, R_2, C_1 and C_2 of the l times filtered KEY image are integrated around the circumference of the ENCRYPTED image. Fig. 7 illustrates the entire encryption process.

5. Visual multimedia content decryption

The decryption process is illustrated in Fig. 8. The following methodology is followed at the receiver site. The two marginal rows and columns are selected from the ENCRYPTED image reaching the receiver. Their content is used to generate the artificial image precisely as described in Section 3. The compact CEDD descriptor is extracted from the artificial image and is searched for in the Compact XML KEY. The values $X-KEY_1[D]$, $X-KEY_2[D]$ and $X-KEY_3[D,Z]$ are retrieved from the file entry in which the distance $D(i,j)$ of the 2 descriptors is zero.

The ENCRYPTED image is separated in $Z\in[0,3]$ non-overlapped square blocks. The CLF-XOR filter is applied $\frac{N}{4}-(X-KEY_3[0,Z])$ times to the red channel, $\frac{N}{4}-(X-KEY_3[1,Z])$ times to the green channel and $\frac{N}{4}-(X-KEY_3[2,Z])$ times to the blue channel of the Z block of the ENCRYPTED image. The procedure is repeated for all the Z blocks. The ENCRYPTED' image is the combination of the four filtered blocks. Then, the CLF-XOR filter is applied $X-KEY_1[D]$ times to the color channels of the KEY image, which is known to the receiver. The resultant image is $\text{KEYimage}_{X-\text{KEY}_1}$. Then the separation process of each color channel of the ENCRYPTED' image is executed according to the following formula (MOD 256):

$$\begin{aligned} &DI[x,y] = EI[x_1+1, y_1+1] - \text{KEYimage}_{X-\text{KEY}_1}[x,y] \\ &x,y\in\{0,N-1\} \\ &x_1,y_1\in\{0,N+1\} \\ &EI[x,y], \text{KEYimage}_{X-\text{KEY}_1}[x,y], DI[x,y]\in\{0,255\} \\ &if\,(DI[x,y]\notin\{0,255\})DI[x,y] = DI[x,y]+255. \end{aligned} \tag{7}$$

The resultant DI image is the DATA image filtered $X-KEY_2[0]$ times on the Red channel, $X-KEY_2[1]$ times on the Green channel and $X-KEY_2[2]$ times on the Blue channel. The DATA image is fully reconstructed by applying the filter CLF-XOR, $\frac{N}{2}-(X-KEY_2[0])$ times to the Red channel of the DI image, $\frac{N}{2}-(X-KEY_2[1])$ times to the Green channel and $\frac{N}{2}-(X-KEY_2[2])$ times to the Blue channel according to the CLF-XOR attribute as described in Section 2.

6. Encryption characteristics

The proposed method is a symmetric private key security method, meaning that the same key is required for encryption and decryption; both sender and receiver must know the key. The key size is the same as the size of the image being encrypted.

It would be rather practical if the proposed method could be classified as a block cipher or stream cipher method. More specifically, a block cipher encryption method applies the KEY on a fixed-length group of bits. For instance, an encryption model of this type would receive a set of n bits plaintext generating a set of n bits cyphertext. The encryption takes place once the system receives the whole n bits set of the plaintext. On the contrary, a stream cipher type model encrypts each bit independently at the moment that it appears.

Considering the proposed method it is obvious that it could not be discretely classified into one of these types of methods. On the one hand, the method depicts similarities with the block cipher method, since the CLF-XOR is applied on blocks of pixels. On the other hand, its application affects only one (the central) pixel of the block, a feature which refer to a stream cipher method. In practice, the method could be defined as *buffered stream cipher* technique, as its application affects only one pixel at a time, but the encryption method implementation requires the buffering of the block pixel values on which the CLF-XOR filter is applied.

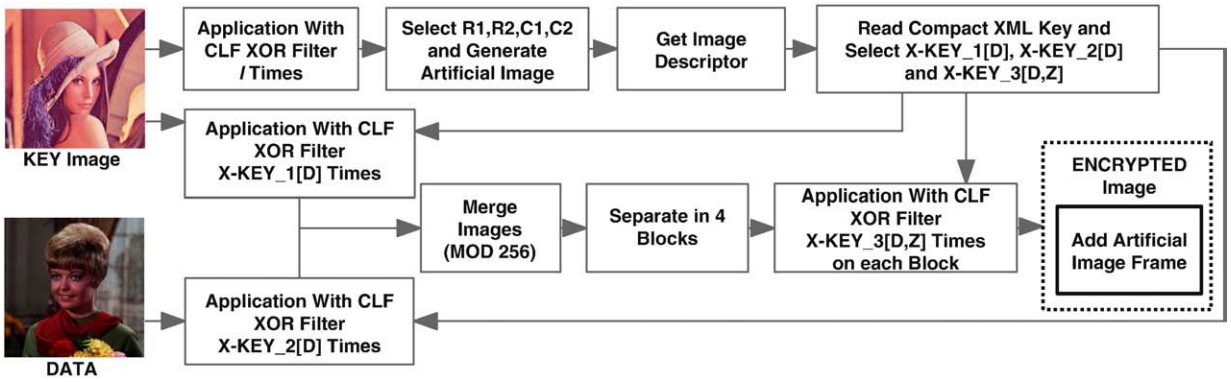

Fig. 7. Encryption process.

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

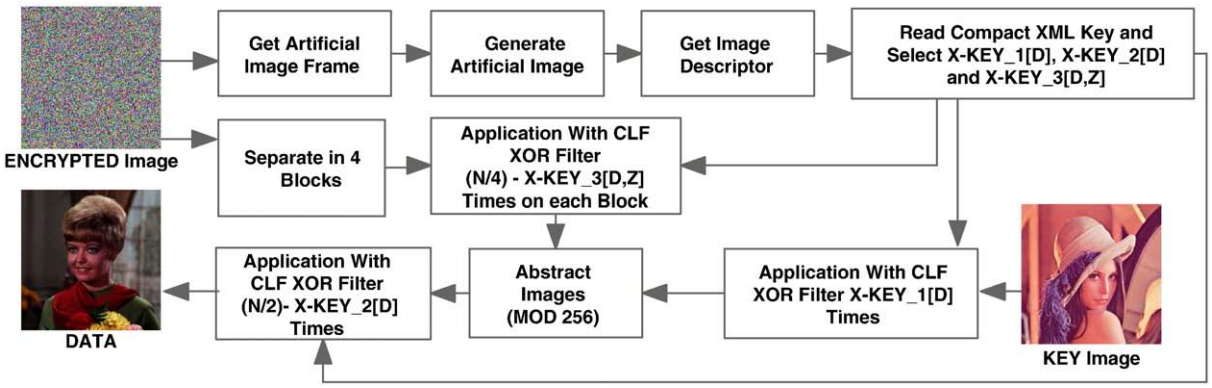

Fig. 8. Decryption process.

6.1. Reasons for using the proposed method

The proposed method exhibits a number of advantages. First of all, the transmission security is guaranteed by the large complexity required in order to obtain access to the data. The conventional encryption methods (block cipher), e.g. the 3DES and AES methods, are incapable of encrypting data with patterns, like images, when used as electronic codebooks (ECB). In order to overcome this problem, cipher block chaining or cipher feedback and output feedback techniques are usually applied. However, in all these cases, their complexity remains considerably smaller contrasted to that of the proposed method.

Moreover, the proposed method is able to approach the excellent, in terms of complexity, results achieved by the traditional OTP method overcoming the constraint of different keys applied for each image. The proposed method can encrypt $\left(\frac{N}{2}-1\right)$ images with the use of just one key.

Furthermore, an important feature that none of the traditional encryption methods exhibits is the capability of the method to produce completely different results for the same images even when the same key is used. The proposed method can be applied to encrypt video transmission e.g. via Internet or cable television. In a video, successive frames may be similar or even identical. The encryption with traditional methods is possible but these successive frames will give the same encrypted image. Watching the scene changes that take place, a kind of scene clustering would be possible in order to obtain the useful information. The encryption with the proposed method, gives different encrypted images even for identical frames. For the case of using the proposed method for video transmission we consider that there will be an exchange of the two keys for a certain number of frames.

In addition, an important feature of the proposed method is its attribute to deteriorate elements of the encrypted image that would possibly reveal information relative with the nature of the image that was encrypted. For illustration we give the example of Fig. 9 on which the same set of keys has been applied in order to encrypt a natural image and a text image. As may be observed from Fig. 9(ii) the brightness histograms of these images are quite different. Nevertheless, after the application of the method, the histograms and other statistical characteristics that come from them tend to coincide.

Furthermore, taking into consideration the implementation of the proposed method in hardware, in terms of circuit design and layout, ease of mask generation, silicon-area utilisation and maximisation of achievable clock speed, CA are perhaps the computational structures best suited for a fully parallel hardware realisation. In contrast to the serial computers, the implementation of the method is motivated by parallelism, an inherent feature of CA that contributes to further acceleration of the model's operation.

It is worth noting that decryption results in a lossless representation of the encrypted image.

A good encryption scheme should withstand all kinds of known attacks. Some security analyses have been performed on the proposed image encryption scheme. The results demonstrate the satisfactory security of the proposed scheme.

6.2. Brute force attack

Brute force attack is a trial and error method of trying every possible combination of characters against the encrypted data in an attempt to retrieve the key. As mentioned above, the security of the proposed image is based on the KEY image. The larger the DATA image, the larger the KEY image which is used. Given that the KEY image is a color image, a very large number of resultant potential security keys are available $([256]^{[N\times N]})^3$. In order to strengthen further the security of the proposed method, the KEY image could be constructed artificially with the method of producing random numbers described in Section 3.

6.3. Known plaintext (DATA image)–Cipher Text (ENCRYPTED image) attack

This form of attack presupposes that the adversary knows a DATA image and ENCRYPTED image pair and is attempting to recover the KEY image. This security test must be used on all encryption schemes that use one key in order to encrypt more than one plaintext (DATA images). In this security test it appears that the Compact XML Key greatly increases the complexity of the method.

Suppose the adversary possesses an ENCRYPTED image produced for a known DATA image with $N\times N$ dimensions. This ENCRYPTED image consists of 4 blocks, for each of which, for each color channel, the CLF-XOR filter has been applied $X-KEY_3[D,Z]$times. Given that the adversary does not know this key, each ENCRYPED image corresponds to

$$\left[\frac{\frac{N}{2}}{2}-1\right]^{12} \tag{8}$$

possible ENCRYPTED' images.

Each ENCRYPTED' image is produced by the combination of each $X-KEY_1[D]$ filtered KEY image and each $X-KEY_2[D]$ filtered DATA image. Given that the DATA image is known, all combinations for the $X-KEY_2[D]$ are tested, which are $\left[\frac{N}{2}-1\right]^3$. Therefore a total of

$$\left[\frac{\frac{N}{2}}{2}-1\right]^{12}\times\left[\frac{N}{2}-1\right]^3 \tag{9}$$

possible $X-KEY_1[D]$ filtered KEY images are produced.

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

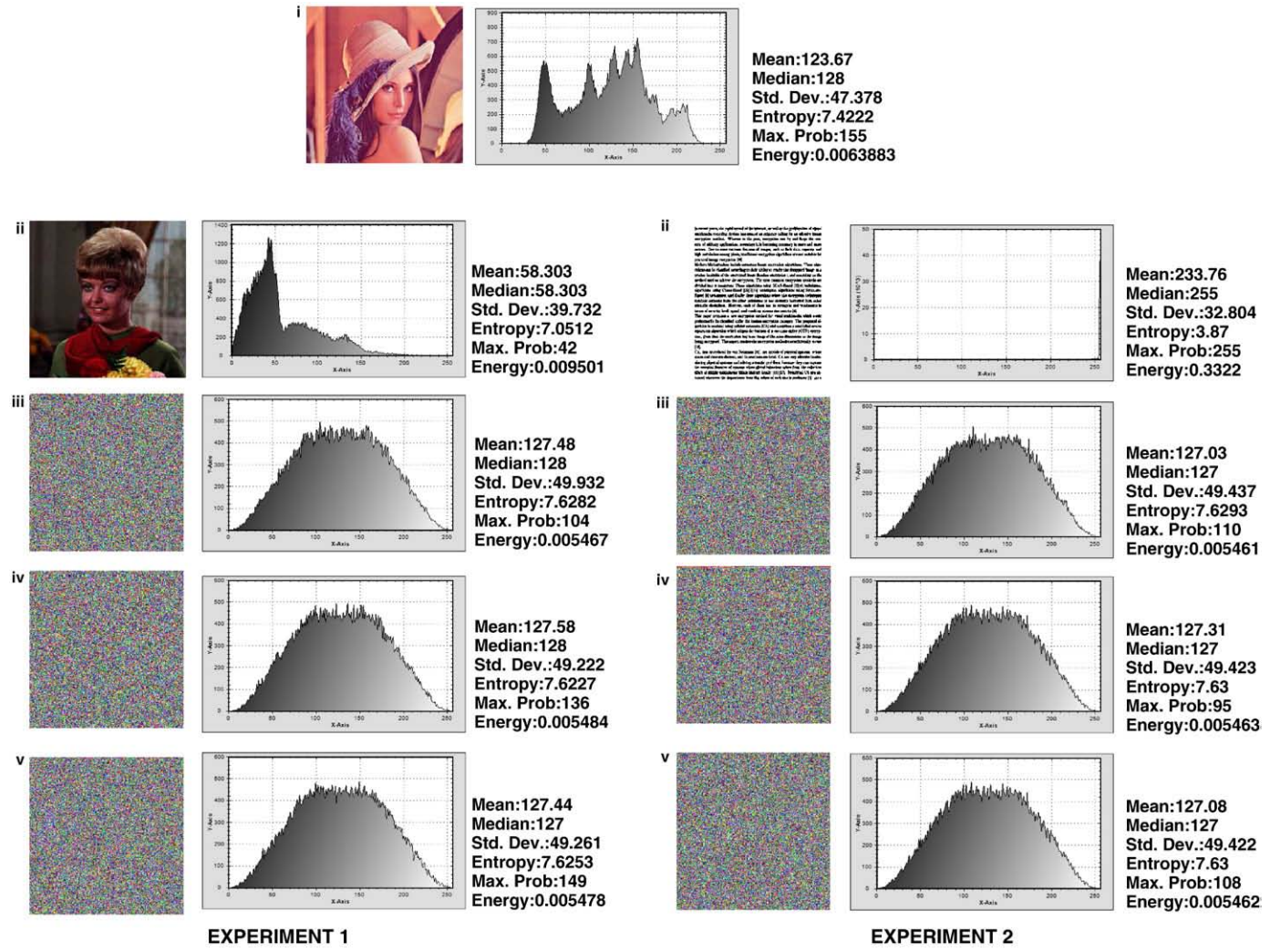

Fig. 9. (i) KEY image, (ii) DATA image and (iii–v) Results of the DATA image encryption using the same KEY image and different set of $X-KEY_1[D]$, $X-KEY_2[D]$ and $X-KEY_3[D,Z]$. The first experiment encrypts a Natural Color image while the second one encrypts an image that represents Text. Observing the characteristics of the resulting luminosity histograms, one can see that each time, the encrypted image is different. Although the two images are quite different (noting both the visual content, as well as the histograms), the distribution of the encrypted image histogram in both experiments is similar. This element enhances the security of the proposed encryption method, since the encrypted image will not disclose any details of the DATA image.

Testing every possible combination for the $X-KEY_1[D]$, which are $\left[\frac{N}{2}-1\right]^3$, it arises that when a DATA image and the corresponding ENCRYPTED image are known there are *Po* possible keys.

$$Po = \left[\frac{\frac{N}{2}}{2}-1\right]^{12} \times \left[\frac{N}{2}-1\right]^3 \times \left[\frac{N}{2}-1\right]^3. \quad (10)$$

For an image with dimensions of 512×512 then 4.8×10^{39} possible keys result. The large number of calculations required makes the method sufficiently secure. Consider the rapid progress of digital computers and distributed arithmetic, the complexity is required to be no lower than $2^{128}=(3.4\times10^{35})$ for strict cipher [46]. The recovery of the KEY image requires yet one more DATA image and ENCRYPTED image pair. Other 4.8×10^{39} possible pairs result, which must be compared with the 4.8×10^{39} possible keys resulting from the first DATA image and ENCRYPTED image pair in order to discover which is the correct key. Therefore, 9.6×10^{39} calculations are needed in order to uncover the KEY image. As mentioned above, the proposed method can be used to transmit encrypted video. During the transmission there shall be an exchange of 2 keys for certain frames. The total calculations that are required to recover the KEY image is exceptionally great and requires an immense computation cost (even if this is distributed on a computational grid) and must be repeated with the same frequency as the key exchange.

6.4. Difference between the ENCRYPTED image and the DATA image

To distinguish the difference between the ENCRYPTED image and the DATA one we adopt the function of peak signal to noise ratio (PSNR). The PSNR is most commonly used as a measure of quality of reconstruction of non-lossless encryption methods [47,48]. However here it is used to measure the difference of the ENCRYPTED image and the DATA one. PSNR is usually expressed in terms of the logarithmic decibel scale.

The PSNR computation method derives from the following equation.

$$PSNR = 20\times log_{10}\left(\frac{(2^n-1)\sqrt{N\times N}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}|DATA(i,j)-ENCRYPTED(i,j)|^2}}\right) \quad (11)$$

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

where N is defined as the square dimension of the images, and n is the number of bits representing a pixel. When using 8 bit images the greatest distance between images is calculated at 0 dB, while when matching the images the value extends infinitely.

The results for the images in Fig. 9 are displayed in Table 1.

Using the CA based random number generator 50 color images constructed. The average PSNR values between the DATA images, used in Fig. 9 and the artificially constructed images are equal to 6.89 dB and 5.36 dB respectively. As one can see, the PSNR results for the ENCRYPTED images and the random generated images are similar. Also, experiments based on WANG [40] image database indicated that the average PSNR is equal to 7.12 dB.

6.5. Partially image decryption when part of the KEY Image is known

In order to study more precisely this scenario, the degree in which the decryption procedure is affected by each pixel of the KEY image should be find out. With the aim of the deeper understanding of the tested model, the encryption and decryption procedures were further simplified by considering that the resulting encrypted image is the ENCRYPTED' and not the ENCRYPTED.

The Lady is encrypted (as depicted in Fig. 10) by using Lena. We modify the XML KEY generation procedure in order to keep the $X-KEY_2[D]$ (that is used for Lady) constant and equal to T while we set $X-KEY_1[D]$ always equal to 1. It is noticed that the whole procedure followed in this section violates the security regulations set for the XML KEY. The purpose of this relaxation is just to assist the evaluation of the DATA Image decryption complexity when part of the KEY Image is known.

Initially, it is assumed that the ENCRYPTED' Image is provided and the DATA Image is requested while the KEY Image is intercepted although missing only one pixel. This pixel could be located in any point of the KEY Image. The images size is 256×256.

Consequently, the way in which the erroneous pixel value affects the KEY Image during the application procedure of the CLF XOR filter in the decryption phase will be investigated. At the first iteration, this pixel causes distortion to the 9 (including this pixel itself) pixels of its neighborhood.

Considering that $T=127$, the decryption of the CLF-XOR filter will be applied only once on the DATA Image (after the KEY Image subtraction).

The result is the DATA Image decryption with a loss of 3^2 pixels. This loss is considered particularly small. However, as long as the $X-KEY_1[D]$ is augmented the loss is also augmented since the content of the surrounding neighborhood was affected during the previous iteration. These happen when $T=127$. In case of a smaller T value, the error also propagates to other areas of the image. Fig. 10 illustrates the image distortion when $T=64$ and $X-KEY_1[D]\in[1,3]$. Apparently the result of the retrieved image is significantly distorted despite the fact that the full KEY Image except one pixel was known. In case of more than 1 pixel loss, the distortion is clearly bigger (especially when the missing pixels don't belong to the same neighborhood).

Theoretically, this scenario doesn't affect the security of the proposed method directly, due to the fact that partial knowledge of the key cannot lead to its full retrieval, but only to the retrieval of a restricted (or even no) part of the DATA image. However, in practice the appeared distortion pattern shapes (Fig. 10) hide information relative to the XML KEY. Assume for example the following attack instance.

Let's consider that a Known Plaintext/Known Cipher Test attack is attempted. The image P is defined as plaintext and the image C as cipher. The attacker tries to decrypt C by using a random image K_1. The result that he/she takes is the E_1. After that, the change of just one pixel of K_1 suffices to take E_2. Observing the patterns on which the changes of the 2 images appear he/she could probably predict the $X-KEY_1[D]$ and $X-KEY_2[D]$ values.

In order to avoid this problem the special concern described in Section 3 should be taken during the Compact XML KEY generation. According to this concern, the three numbers that configure the $X-KEY_1[D]$ and $X-KEY_2[D]$ shouldn't contain the same number three times. That is, the equalities $X-KEY_1[0]=X-KEY_1[1]=X-KEY_1[2]$ and $X-KEY_2[0]=X-KEY_2[1]=X-KEY_2[2]$ should never hold. Having this constraint satisfied, a complex distortion distribution – exceptionally difficult to model – is achieved. A single pixel distortion in the aforementioned attack scenario, leads to image distortion, constant every time though, that could be coming from any possible pair of $X-KEY_1[D]$ and $X-KEY_2[D]$. As depicted in Fig. 10, then non-knowledge of a single pixel causes big distortions to the retrieved images.

6.6. Is the proposed method unconditionally secure?

Each encryption method certainly has its weaknesses. The present method features the following problems, which may be covered in future work.

First of all, the proposed method can be applied only if the resolution of the images is a power of 2. This weakness can be easily overcome by modifying the images using (adding) extra pixels as frame in order to accomplish the correct dimension.

If the adversary attempts a chosen plaintext (DATA image) attack using one monochrome image, the method has the following weakness: The application of the $X-KEY_2[D]$ to the DATA image does not cause any change in the content of the image. Suppose the image has $N\times N$ dimensions and all the pixels a value of $(0,0,0)$. The ENCRYPTED' image consists in reality only of the filtered $X-KEY_1[D]$ times KEY image. The separation of the image into blocks and the application of the $X-KEY_3[D,Z]$ key may change the KEY image substantially but its recovery does not require so many calculations as it appears than those required to recover the key in the case of a known plaintext (DATA image)–Cipher Text (ENCRYPTED image) attack. Can this problem be overcome? One initial technique which reinforces the security of the proposed method is the following: After the completion of the production of the ENCRYPTED image and before the Artificial image Frame is added, the ENCRYPTED image shall participate in yet one more MOD 256 action with the $X-KEY_1[D]$ times filtered KEY image. This technique, which does not cause much change to the proposed schema, significantly increases the calculations that are required to recover the key also in the case of a known plaintext (DATA image)–Cipher Text (ENCRYPTED image) attack.

Furthermore, the proposed method has the following weakness: The successful recovery of part of the KEY results in the recovery of part of the DATA image. Can this problem be overcome? An initial scenario for solving this problem is that the KEY image first

Table 1
PSNR values for the encrypted images of Fig. 9, per color channel.

Color Channel	Experiment 1		Experiment 2	
	Encrypted image	PSNR	Encrypted image	PSNR
Red Channel	(iii)	8.11 dB	(iii)	4.99 dB
Green Channel		7.03 dB		5.59 dB
Blue Channel		6.81 dB		5.61 dB
Average PSNR		7.32 dB		5.40 dB
Red Channel	(iv)	8.12 dB	(iv)	5.01 dB
Green Channel		7.04 dB		5.49 dB
Blue Channel		6.83 dB		5.22 dB
Average PSNR		7.33 dB		5.24 dB
Red Channel	(iv)	8.08 dB	(iv)	5.11 dB
Green Channel		7.04 dB		5.03 dB
Blue Channel		6.81 dB		4.87 dB
Average PSNR		7.31 dB		5.00 dB
Random images	DATA	6.89 dB	DATA	5.36 dB

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

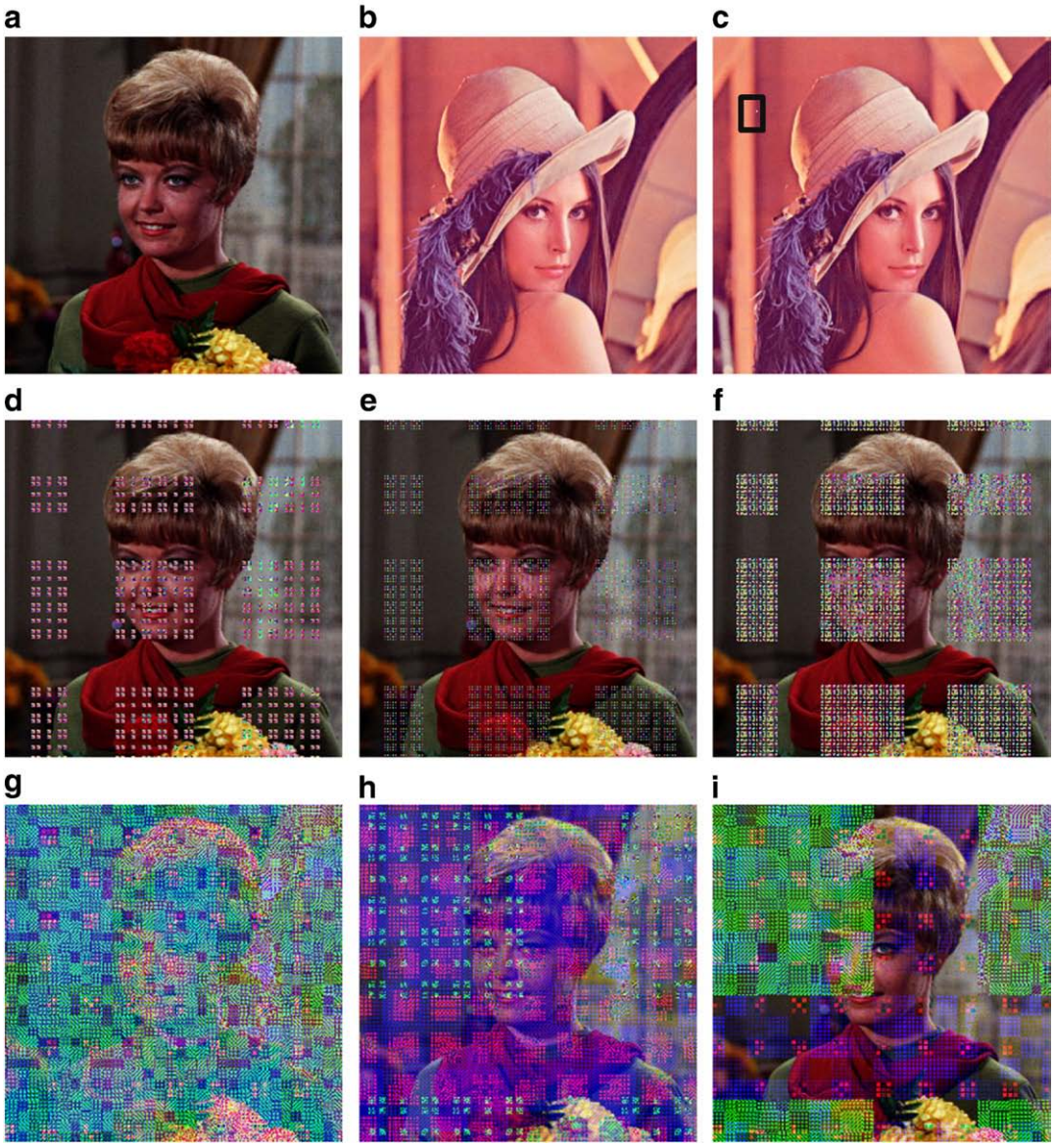

Fig. 10. (a) Lady-DATA Image, (b) Lena-KEY Image, (c) Lena with one pixel lost, (d) image decryption with $X-KEY_1[D]=1$ and $X-KEY_2[D]=64$, (e) image decryption with $X-KEY_1[D]=2$ and $X-KEY_2[D]=64$, (f) image decryption with $X-KEY_1[D]=3$ and $X-KEY_2[D]=64$, (g) image decryption with $X-KEY_1[0]=100, X-KEY_1[1]=25, X-KEY_1[2]=80$ and $X-KEY_2[0]=63, X-KEY_2[1]=25, X-KEY_2[2]=65$, (h) image decryption with $X-KEY_1[0]=100, X-KEY_1[1]=25, X-KEY_1[2]=80$, and $X-KEY_2[0]=25, X-KEY_2[1]=63, X-KEY_2[2]=65$, (i) image decryption with $X-KEY_1[0]=100, X-KEY_1[1]=25, X-KEY_1[2]=80$, and $X-KEY_2[0]=63, X-KEY_2[1]=65, X-KEY_2[2]=25$.

participates in one of the processes for the Structure-Based changes and then interacts with the DATA image.

One extra security test would be the scenario of the XML KEY interception while the encrypted image is also known. Actually, this scenario could be divided into 2 sub-scenarios. Initially the case considered is that the attacker knows part of the KEY while in the second scenario the attacker is aware of the entire file. Every ENCRYPTED image contains the information required to reconstruct the Artificial Image. The CEDD descriptor could be obtained by anyone, as long as its extraction algorithm for this image is given. Let's consider that someone knows just one entry of the XML KEY. The probability of this entry being the one which corresponds to the descriptor is quite big. Therefore, the attacker will probably have access to the $X-KEY_1[D]$, $X-KEY_2[D]$, and $X-KEY_3[D,Z]$. This fact doesn't reduce the method's complexity. In fact, the complexity remains at Brute Force Attack levels, since the retrieval of the DATA image requires the prediction of the KEY image. The situation changes dramatically when the attacker knows more than one XML KEY entries.

The second scenario considers the case of 2 or more XML KEY entries known to the attacker while he/she has access to at least 2 ENCRYPTED images. In this case, he/she can extract the descriptor from these 2 images and take the corresponding $X-KEY_3[D,Z]$ values. Applying the procedure described in Section 5 he can obtain the 2 ENCRYPTED images. A reminder should be given at this point for the Compact XML KEY generation algorithm parameter mentioned in Section 3: Not equal values should be assigned to $X-KEY_1[D]$ and $X-KEY_2[D]$. In other case, the attacker could get access to the KEY image indirectly by using the relationship of Eq. (7). The constraint for unequal $X-KEY_1[D]$ and $X-KEY_2[D]$ values theoretically protects the method. This is due to the fact that in order to obtain access to the DATA image someone would need to detect the KEY image KEY image via a Brute Force Attack. Things get worse when the user, along with the knowledge either of a part or of the whole key, attempts to known the plaintext/Cipher text. In this case the proposed method exhibits the OTP weaknesses during which the same key is used for more than one times. It is noted that this disadvantage appears when the key is

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043

intercepted. If somebody attempts to create an XML KEY artificially while he knows a pair of DATA image/ENCRYPTED image, the method complexity is equal to the one estimated for the Known Plain Text Attack scenario.

7. Conclusions

This paper presented a visual multimedia content encryption model using CA. The method combines two keys for the encryption. The first Key is an image of the same dimensions as the image being encrypted while the second one results from the structure of an artificial image produced by the superposition of four 1-D CA time–space diagrams as well as from a CA based random number generator. Decryption results in a lossless representation of the encrypted image. Image retrieval techniques are employed in order to accelerate the process of decryption. One of the most important characteristics of the proposed method is that the resulting encrypted image for a given key image, using the same key image is different each time. Experimental results have shown that the encrypted images that result do not contain statistical information that could reveal the source from which they originate. Moreover, the proposed methods appear to be able to withstand brute force attacks and the known plaintext (DATA image)–Cipher Text (ENCRYPTED image) attack. The potential weaknesses of this method may be the focus of future work. The proposed method is implemented in C# and is available online through the img(Rummager)[1] [49] application.

References

[1] G.-J. Xiao, H.-P., Zhang, Proc. International Conference on Machine Learning and Cybernetics, 2006, p. 2707.
[2] N. Bourdakis, C. Alexopoulos, Pattern Recognition Vol. 25 (6) (1992) 567 25.
[3] R.-J. Chen, W.-K. Lu, J.-L. Lai, IEEE International Symposium on Circuits and Systems ISCAS 2005, 2005, p. 1690.
[4] J. Scharinger, Electronic Imaging 17 (2) (1998) 318.
[5] T. Gaoand, Z. Chen, Physics Letters A 372 (4) (2008) 394 21.
[6] S.Koduru, V.Chandrasekaran, Integrated confusion–diffusion mechanisms for chaos based image encryption (2008) 260–263.
[7] K. Chung, L. Chang, Pattern Recognition Letters 19 (5–6) (1998) 461.
[8] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of applied cryptography, CRC press, 1997.
[9] J. Von Neumann, A. Burks, et al., Theory of self-reproducing automata, University of Illinois Press, Urbana, 1966.
[10] R. Feynman, International Journal of Theoretical Physics 21 (6) (1982) 467.
[11] S. Wolfram, Advanced Series on Complex Systems, World Scientific Publication, Singapore, 1986.
[12] A. Adamatzky, Identification of cellular automata, CRC Press, 1994.
[13] B. Chopard, M. Droz, Cellular automata modeling of physical systems, Cambridge University Press, New York, 1998.
[14] T. Toffoli, Physica D: Nonlinear Phenomena 10 (1984) 1.
[15] I. Bialynicki-Birula, Physical Review D 49 (12) (1994) 6920.
[16] S. Omohundro, Physica D: Nonlinear Phenomena 10 (1984) 1.
[17] B. Malamud, D. Turcotte, Computing in Science & Engineering 2 (3) (2000) 42.
[18] G. Sirakoulis, I. Karafyllidis, V. Mardiris, A. Thanailakis, Nanotechnology 10 (1999) 421.
[19] G. Sirakoulis, I. Karafyllidis, A. Thanailakis, Ecological Modelling 133 (3) (2000) 209.
[20] G. Sirakoulis, I. Karafyllidis, A. Thanailakis, V. Mardiris, Advances in Engineering Software 32 (3) (2000) 189.
[21] G.C. Sirakoulis, I. Karafyllidis, A. Thanailakis, Microprocessors and Microsystems 27 (8) (2003) 381.
[22] G. Sirakoulis, Integration, the VLSI Journal 37 (1) (2004) 63.
[23] V. Mardiris, G.C. Sirakoulis, C. Mizas, I. Karafyllidis, A. Thanailakis, IEEE Trans. SMC-Part C 2 (38) (2008) 1.
[24] R. Chen, J. Lai, Proceedings of the 2002 IEEE Asia-Pacific Conference on Circuit and Systems, Vol. 2, 2002, p. 279, APCCAS'02.
[25] R. Chen, J. Lai, Y. Lai, Proceedings of the 7th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol. 12, 2003, p. 165, SCI 2003.
[26] S. Maniccam, N. Bourbakis, Pattern Recognition 34 (6) (2001) 1229.
[27] I. Karafyllidis, I. Andreadis, P. Tzionas, P. Tsalides, A. Thanailakis, Pattern Recognition 29 (4) (1996) 689.
[28] F. Seredynski, P. Bouvry, A. Zomaya, Parallel Computing 30 (5–6) (2004) 753.
[29] O. Lafe, Engineering Applications of Artificial Intelligence 10 (6) (1997) 581.
[30] P. Guan, Complex Systems 1 (1987) 51.
[31] J.Kari, Cryptosystems based on reversible cellular automata, Personal communication.
[32] R. Chen, J. Lai, Pattern Recognition 40 (5) (2007) 1621.
[33] P. Dasgupta, S. Chattopadhyay, P. Chaudhuri, I. Sengupta, IEEE Transactions on Computers 50 (2) (2001) 177.
[34] B. Mertzios, K. Tsirikolias, Logic Filters: Theory and Applications, Nonlinear Image Processing, Chapter 11, Academic Press, ISBN: 0125004516, 2004.
[35] B.Mertzios, K.Tsirikolias, Applications of coordinate logic filters in image analysis and pattern recognition, IEEE Service Center.
[36] L. Gray, Notices-American Mathematical Society 50 (2) (2003) 200.
[37] S. Chatzichristofis, Y. Boutalis, Lecture Notes in Computer Science (LNCS), 5008, Springer, 2008, p. 312, Vol.
[38] S.A. Chatzichristofis, K. Zagoris, Y.S. Boutalis, N. Papamarkos, International Journal of Pattern Recognition and Artificial Intelligence 24 (2) (2010) 207 IJPRAI.
[39] S. Chatzichristofis, Y. Boutalis, IASTED International Conference on Artificial Intelligence and Soft Computing (ASC 2007), 2007, p. 280.
[40] J. Wang, J. Li, G. Wiederhold, IEEE Transactions on Pattern Analysis and Machine Intelligence 23 (9) (2001) 947.
[41] L. Kotoulas, D. Tsarouchis, G. Sirakoulis, I. Andreadis, IEEE International Symposium on Circuits and Systems, ISCAS 2006. Proceedings, 2006, p. 4627.
[42] A. Rukhin, NIST special publication, US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2000.
[43] S. Chatzichristofis, Y. Boutalis, Multimedia Tools and Applications (2009) 1.
[44] S. Chatzichristofis, Y. Boutalis, M. Lux, Proceedings of the 6th IASTED International Conference, Vol. 134643, 2008, p. 064.
[45] S. Chatzichristofis, Y. Boutalis, Proceedings of the 9th International Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS, 2008, p. 191.
[46] B. Schneier, Applied Cryptography, Second edition, JohnWiley and Sons Inc, 1996.
[47] Z. Liu, M. Ahmad, S. Liu, Optics Communications 281 (2008) 5322.
[48] C. Shin, S. Kim, Optics Communications 254 (1–3) (2005) 67.
[49] S. Chatzichristofis, Y. Boutalis, M. Lux, 2nd International Workshop on Similarity Search and Applications, IEEE Computer Society, Prague, Czech Republic, 2009, p. 151, SISAP.

[1] http://www.img-rummager.com.

Please cite this article as: S.A. Chatzichristofis, et al., A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. (2010), doi:10.1016/j.optcom.2010.06.043