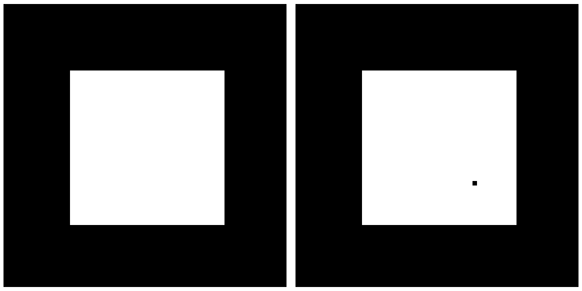

(a) Original image. (b) Modified image.

Fig. 2. Hash of some black and white images.

C. *Application example*

Let us consider the two black and white images of size 64×64 in Fig. 2, in which the pixel in position (40,40) has been changed. In this case, our hash function returns:

```
34A5C1B3DFFCC8902F7B248C3ABEFE2C
9C9538E5104D117B399C999F74CF1CAD
```

for the Fig. 2(a) and

```
5E67725CAA6B7B7434BE57F5F30F2D3D
57056FA960B69052453CBC62D9267896
```

for the Fig. 2(b).

Let us consider now the two 256 graylevel images of Lena (256×256 pixels) in figure 3, in which the grayscale level of the pixel in position (50,50) has been transformed from 93 (fig. 3(a)) to 94 (fig. 3(b)). In this case, our hash function returns:

(a) Original lena. (b) Modified lena.

Fig. 3. Hash of some grayscale level images.

```
FA9F51EFA97808CE6BFF5F9F662DCD73
8C25101FE9F7F427CD4E2B8D40331B89
```

for the left Lena and

```
BABF2CE1455CA28F7BA20F52DFBD24B7
6042DC572FCCA4351D264ACF4C2E108B
```

for the right Lena.

These examples give an illustration of the avalanche effect obtained by this algorithm. A more complete study of the properties possessed by our hash functions and resistance under collisions will be studied in future work.

VI. CONCLUSION

In this paper, a new approach to generate algorithms with chaotic behaviors is proposed. This approach is based on the well-known Devaney's topological chaos. The algorithms which are of iterative nature are based on the so-called chaotic iterations. This is achieved by establishing a link between the notions of topological chaos and chaotic iterations. This is the first time that such an approach is considered for chaotic iterations. Indeed, we are not interested in stable states of such iterations as it has always been the case in the literature, but in their unpredictable behavior. After a solid theoretical study, we consider the practical implementation of the proposed algorithms by evaluating the case of finite sets. We study the behavior of the induced computer programs proving that it is possible to design true chaotic computer programs. A simple application is proposed in the area of hash functions. The security in this case is defined by the unpredictability of the behavior of the proposed algorithm. The algorithm derived from our approach satisfies important properties of topological chaos such as sensitivity to initial conditions, uniform repartition (as a result of the transitivity), and unpredictability. The results expected in our study have been experimentally checked. The choices made in this first study are simple: the aim was not to find the best hash function, but to give simple illustrated examples to prove the feasibility in using the new kind of chaotic algorithms in computer science. In future work, we will investigate other choices of iteration functions and chaotic strategies. We will try to characterize transitive functions. Other properties induced by topological chaos, such as entropy, will be explored and their interest in the information security framework will be shown.

REFERENCES

[1] J. M. Bahi and S. Contassot-Vivier. Stability of fully asynchronous discrete-time discrete state dynamic networks. *IEEE Transactions on Neural Networks*, 13(6):1353–1363, 2002.

[2] J. Banks, J. Brooks, G. Cairns, and P. Stacey. On devaney's definition of chaos. *Amer. Math. Monthly*, 99:332–334, 1992.

[3] Jin Cong, Yan Jiang, Zhiguo Qu, and Zhongmei Zhang. A wavelet packets watermarking algorithm based on chaos encryption. *Lecture Notes in Computer Science*, 3980:921–928, 2006.

[4] Zhao Dawei, Chen Guanrong, and Liu Wenbo. A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons and Fractals*, 22:47–54, 2004.

[5] Robert L. Devaney. *An Introduction to Chaotic Dynamical Systems, 2nd Edition*. Westview Pr (Short Disc), March 2003.

[6] Peng Fei, Qiu Shui-Sheng, and Long Min. A secure digital signature algorithm based on elliptic curve and chaotic mappings. *Circuits Systems Signal Processing*, 24, No. 5:585–597, 2005.

[7] Shao-Hui Liu, Hong-Xun Yao, Wen Gao, and Yong-Liang Liu. An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. *Applied Mathematics and Computation*, 185:869–882, 2007.

[8] F. Peng, S.-S. Qiu, and M. Long. One way hash function construction based on two-dimensional hyperchaotic mappings. *Acta Phys. Sinici.*, 54:98–104, 2005.

[9] F. Robert. *Discrete Iterations: A Metric Study*, volume 6 of *Springer Series in Computational Mathematics*. 1986.

[10] Chang song Zhou and Tian lun Chen. Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. *Physics Letters A*, 234(6):429 – 435, 1997.