Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Digital image encoding using hyperchaos

F. Belkhouche and I. Gokcen
Email: fet_blk@yahoo.fr

***Abstract*—In this paper we present a digital gray-level image encoding method based on hyperchaotic maps, which have positive Lyapunov exponents in more than one direction and can be combined with an algebraic output equation. 2D and 3D maps are used to perform pixel value and pixel position permutation simultaneously. The sensitivity to the initial states guarantees the diffusion property where local pixels spread out on the entire image and become uncorrelated. Our experiments illustrate that 2D and 3D hyperchaotic maps with large key spaces improve both the diffusion and confusion properties compared to chaotic maps. Parallel encoding is also discussed for large-scale images.**

***Index Terms*—Hyperchaos, image encoding.**

I. Introduction

Information security has been a critical problem in several areas such as the Internet applications, computer networks and communications. Potentially any area where information needs to be protected from being disclosed to unauthorized parties can benefit from secure transmission and processing of information. Various encryption algorithms have been proposed to perform this task in the past [1]. Recently, a new class of encryption methods utilizing the dynamics of chaos has been proposed [2].

Chaos has found application areas in secure analog communications since the early 1990s and most of the developed algorithms have been based on chaos synchronization and chaos shift keying [3], [4], [5], [6]. The fundamental concepts in chaos theory such as the sensitivity to initial conditions and measure-preserving transformation can be applied to cryptography. For instance the sensitivity to initial conditions property of chaos can satisfy the diffusion requirement. Besides the secure analog communication algorithms, digital chaotic algorithms have also been developed, particularly for text encryption. As an example, Babtista's method utilizes the number of iterations of the well-known Logistic map where a portion of the attractor generated by the map is associated with a text unit [7]. Encryption then consists of executing the required number of iterations to reach a region, which corresponds to a specific text unit.

Although, there are ample chaotic methods for text encryption, their applications to images are not straightforward due to the characteristics of images and the added complexity. For example, the memory required to store images is much higher and most real-time text encryption algorithms do not work efficiently for image encryption tasks. Therefore, novel methods using chaotic maps have been developed recently for image encoding and transformation [8], [9], [10], [11]. Two prominent examples are the one-dimensional piecewise linear Baker map [12] and the Logistic map [13]. Gao et al. pointed to the drawbacks of piecewise linear maps and introduced a highly non-linear version of the Logistic map as a remedy [14]. Since non-linear Logistic map inherits some properties of its predecessor, Behnia et al. mixed a coupled map with a one-dimensional chaotic map for improved security [15]. Ahmed et al. introduced another Logistic map variant and combined it with an independent feedback mechanism to implement a stream cipher for image encryption [16]. Parallel image encryption and general design rules to improve chaos-based systems have also been discussed in the literature [17], [18].

In spite of the variety of chaotic image encryption systems, there have been very few attempts to use hyperchaos for image encoding [19]. We aim at bridging this gap and develop algorithms with iterative maps, which may have non-chaotic output equations. We couple position and value permutations in this paper and validate the efficacy of our formulation with experiments. Our contributions can be summarized as follows:

- Introduction of multi-dimensional hyperchaotic maps to combine pixel value and position transformations
- A simple algorithm to parallelize the slow sequential encoding
- Enhanced security with N-level transformations

Due to limited space, we will describe the contributions in general in this paper and defer the detailed descriptions to a future publication.

The paper is organized as follows. In the next section we describe the hyperchaotic image encoding model and introduce the maps. Section 3 discusses the parallelization and N-level transformations and finally we conclude with a summary of the results and future research directions.

II. Model description

A gray scale image can be mathematically described as a graph of a function representing the intensity level or the brightness of the image and its support. Encoding algorithms can act on the support of the image or on the intensity level itself. In this paper, we present gray-level image encoding using a class of non-linear dynamical systems. Since we are dealing with digital images, we use a discrete-time dynamical system. The algorithms can easily be extended to color images by making use of the juxtaposition of three layers representing gray scale images. Because of the nature of the digital images, the encoding algorithm can act on the pixel value $L_p \in [0, 255]$, or the pixel's position $P = (P_x, P_y)$. It is also possible to act on the pixel's value and position simultaneously. If P denotes the initial image, X denotes the image in the hyperchaoric attractor, and Y denotes the transformed image, the transformation to associate each pixel value in P to another

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

pixel value in Y can be given as $\phi : P \times a \longrightarrow Y$ or $Y = \phi(P, a)$, where a is a set of real control parameters. In our formulation, ϕ is the algorithm that establishes the image transformation. The block encoding algorithm can be written as an initial value discrete-time dynamical system as follows

$$\begin{aligned} x(k+1) &= f(x(k), r) \\ y(k+1) &= g(x(k+1), h) \\ x(k=0) &= x(0) \end{aligned} \tag{1}$$

where $x(k) = [x_1(k), ..., x_n(k)]^T$ is the state vector, and $x(k = 0) = [x_1(0), ..., x_n(0)]^T$ is the initial state. Vectors r and h are vectors of real parameters and $y(k) = [y_1(k), ..., y_m(k)]^T$ is the output vector. Functions f and g are nonlinear mappings. The y-equation is the algebraic output equation, n is the state space dimension and m is the output vector dimension. The initial state $x(0)$, the set of parameters a and the nonlinear mappings f and g are chosen so that the aforementioned dynamical system exhibits hyperchaotic behavior, which implies that the system has at least two positive Lyapunov exponents. This is sufficient to satisfy the diffusion property i.e., the property of spreading out a single initial state over many final states, where the orbits starting from an initial state inside the attractor will diffuse and cover the entire region in the phase plane where the attractor lies. The set of parameters, the initial conditions and the hyperchaotic map are parts of the transformation ϕ. Since an image is transformed using a dynamical system, it is represented by real values instead of integers. Initial state as well as the nonlinear map parameters are therefore real numbers, which enhances the encryption security. Note that chaotic encryption suffers from the sensitivity to initial conditions and it becomes more pronounced when we try to recover the initial state using the inverse of the chaotic map. As such chaotic encryption needs some precaution. In our formulation, we do not use the inverse map. Instead the initial image is recovered using the original map and with the help of the keys. Special forms of system (1) that are of particular interest in this paper are as follows:

$$\begin{aligned} x_1(k+1) &= f_1(x_1(k), x_2(k), r) \\ x_2(k+1) &= f_2(x_1(k), x_2(k), r) \\ y_1(k+1) &= g(x_1(k+1), x_2(k+1), h) \\ x(k=0) &= x(0) \end{aligned} \tag{2}$$

and

$$\begin{aligned} x_1(k+1) &= f_1(x_1(k), x_2(k), x_3(k), r) \\ x_2(k+1) &= f_2(x_1(k), x_2(k), x_3(k), r) \\ x_3(k+1) &= f_3(x_1(k), x_2(k), x_3(k), r) \\ x(k=0) &= x(0) \end{aligned} \tag{3}$$

As before, these maps have to satisfy the condition on the Lyapunov exponents. Our encoding algorithm uses a very large key space due to the initial real state vector values being used as a part of the key. Large key space ensures safety against brute-force attacks. Figure 1 illustrates the diffusion property and the sensitivity to the initial states. The initial image is a 9 by 9 pixel image with three levels of gray with a gray horizontal line and white vertical line in a black square. The transformed images are shown in figure 1–b,c,d. It is clear that the local pixels spread out on the entire image and become uncorrelated. The images in figure 1-b, 1-c and 1-d are obtained from initial states $[x_1(0), x_2(0)] = [0.21, 0.2]$, $[x_1(0), x_2(0)] = [0.2, 0.2]$ and $[x_1(0), x_2(0]) = [0.2000000001, 0.2]$, respectively. It is clear that the transformed images are different even though their initial states are very similar. This is due to the sensitivity to the initial states of the hyperchaotic map, where close orbits separate exponentially. When the initial states are extremely similar, the resulting images may exhibit correlation (e.g. Figure 1-c and 1-d).

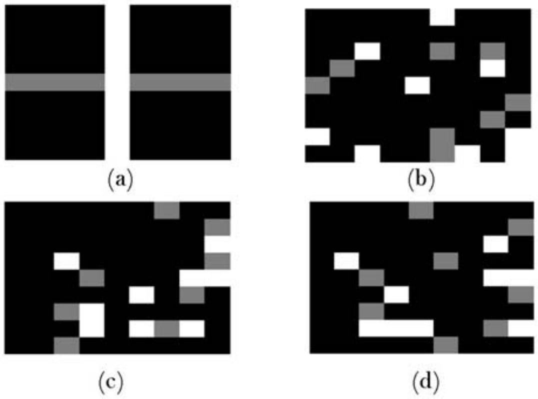

Fig. 1. An illustration of the diffusion property and the sensitivity to the initial states. (a): Three-level 9 by 9 pixels image with a gray horizontal line and white vertical line. (b),(c),(d): the same image transformed using a hyperchaotic map from different but very close initial conditions.

A. Encoding using 2D hyperchaotic maps with an algebraic output equation

The general form is given by the system (2) and various 2D hyperchaotic maps can be used. In this paper, we suggest to use the generalized sine map given by

$$\begin{aligned} &x_1(k+1) = r_1 x_2(k) \\ &x_2(k+1) = r_2 \sin(x_1(k)) \\ &y_1(k) = h_1 x_1(k) + h_2 x_2(k) \end{aligned} \tag{4}$$

where $r = [r_1, r_2]$ is a real-valued vector. A sketch of the attractor is shown in figure 2, which illustrates the ergodicity property and the chaotic solution goes through all of the states in the phase plane. System (4) allows to perform the pixel position and value encoding in a coupled manner, where two of the three variables (x_1, x_2, y_1) are assigned to the pixel position and the third variable is assigned to the pixel value.

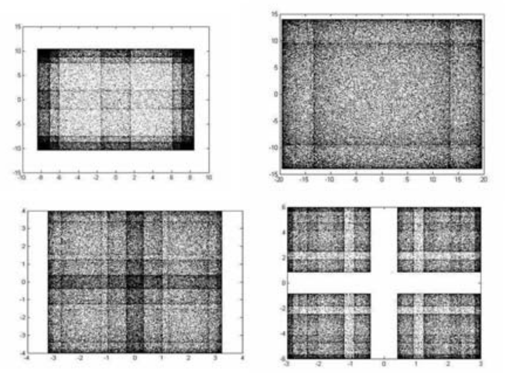

Fig. 2. Hyperchaotic attractor for various values of the control parameters

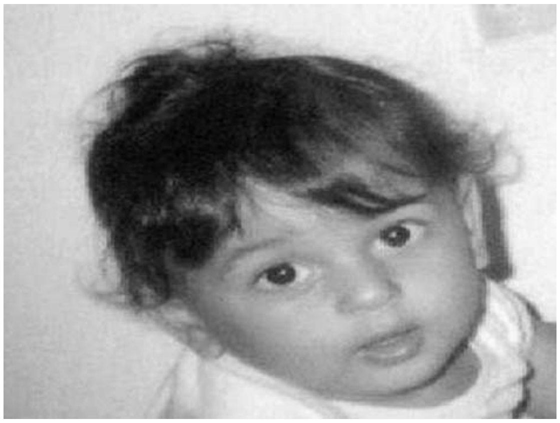

Fig. 3. Original image

B. Encoding using 3D hyperchaotic maps

The general form is given by the system (3). In this paper, we suggest to use the generalized Hénon map given by

$$\begin{aligned} x_1(k+1) &= r_1 - x_2^2(k) - r_2 x_1(k) \\ x_2(k+1) &= x_1(k) \\ x_3(k+1) &= x_2(k) \end{aligned} \tag{5}$$

A hyperchaotic behavior is obtained with $r_1 = 3.4$ and $r_2 = 0.1$. The suggested algorithms combine pixel's position and the pixel's value for encoding. Image transformation using the system (4) is shown in figures 3 and 4. Hyperchaotic map transformations allow confidentiality and data preservation. This can be observed from the histogram of the transformed image, which is the same as the histogram of the original image.

III. PARALLELIZATION AND BLOCK TRANSFORMATION

Encoding very large images could be problematic because it becomes difficult to speed up the permutation process. To solve this problem we suggest to use parallelization and block transformation. A large image can first be segmented into blocks of equal size and then blocks can be encoded in parallel. To that end, any of the hyperchaotic maps presented in this paper can be used for block encoding, similar to the way the map would transform a single image. Various parallelization algorithm can be used. One particular case is to use data parallelism algorithm, which distribute the data across different processors and process the data in parallel. Different maps with different keys can be sued for each loop. The calculations are quite the same for all the loops.

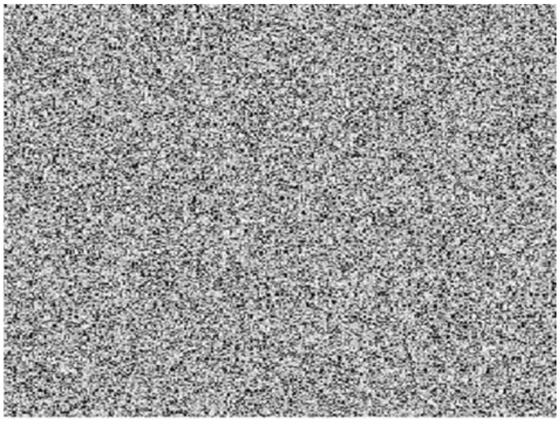

Fig. 4. Image transformed using hyperchaos

IV. CONCLUSION

In this paper, we presented an image encoding method using hyperchaotic dynamical systems and several maps to combine pixel value and position. Being more sensitive to the initial conditions than their chaotic counterparts, hyperchaotic maps exhibit better confusion and diffusion properties. We also introduced the use of parallel encoding for large size images and N-level transformations to improve the security of the algorithm. Preliminary experimental results illustrate the efficacy of our method and its data-preserving nature. Future research areas include devising efficient parallel encoding algorithms and new hyperchaotic maps to extend the methods presented in this paper.

REFERENCES

[1] A. Uhl and A. Pommer, "Image and video encryption: From digital rights management to secured personal communication," *Advances in information security*, vol. 15, 2005.

[2] B. Furht and D. Kirovski, "Multimedia security handbook," *CRC PRESS*, 2005.

[3] G. Perez and H. Cerdeira, "Extracting messages masked by chaos," *Physical Review Letters*, vol. 74, pp. 1970–1973, 1995.

[4] K. Short, "Steps toward unmasking secure communication," *International Journal of Bifurcation and Chaos*, vol. 4, pp. 959–977, 1994.

[5] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys Review Letters*, vol. 64, pp. 821–824, 1990.

[6] H. Guojie, F. Zhengjin, and M. Ruiling, "Chosen ciphertext attack on chaos communication based on chaotic synchronization," *IEEE Trans Circuits and Systems*, vol. 50, pp. 275–279, 2003.

[7] S. Babtista, "Cryptography with chaos," *Physical Letters A*, vol. 240, pp. 50–54, 1998.

[8] G. Gu and G. Han, “An enhanced chaos based image encryption algorithm,” in *First International Conference on Innovative Computing, Information and Control*, vol. I. ICICIC, 2006, pp. 492–495.

[9] Z. Han, W. X. Feng, L. Z. Hui, L. D. Hai, and L. Y. Chou, “A new image encryption algorithm based on chaos system,” in *International Conference on Robotics, Intelligent Systems and Signal Processing*. IEEE, 2003, pp. 778–782.

[10] F. Huang and Y. Feng, “An image encryption approach based on a new two-dimensional map,” in *International Conference on Intelligent Information Hiding and Multimedia*, 2006, pp. 125–130.

[11] J.-L. Fan and X.-F. Zhang, “Image encryption algorithm based on chaotic system,” in *International Conference onComputer-Aided Industrial Design and Conceptual Design*. CAIDCD, 2006, pp. 1–6.

[12] M. Salleh, S. Ibrahim, and I. Isnin, “Enhanced chaotic image encryption algorithm based on bakerapos’s map,” in *International Symposium on Circuits and Systems*, vol. II. IEEE, 2003, pp. 508–511.

[13] N. Pareek, V. Patidar, and K. Sud, “Image encryption using chaotic logistic map,” *Image and Vision Computing*, vol. 24, pp. 926–634, 2006.

[14] H. Gao, Y. Zhang, S. Liang, and D. Li, “A new chaotic algorithm for image encryption,” *Chaos, Solitons and Fractals*, vol. 29, pp. 393–399, July 2005.

[15] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, “A novel algorithm for image encryption based on mixture of chaotic maps,” *Chaos, Solitons and Fractals*, vol. 35, pp. 408–419, 2008.

[16] H. Ahmed, H. Kalash, and O. FaragAllah, “An effecient chaos-based feedback stream cipher for image encryption and decrytion,” *Informatica*, vol. 31, pp. 121–129, 2005.

[17] Q. Zhou, K. Wong, X. Liao, T. Xianf, and Y. Hu, “Parallel image encryption algorithm based on discretized choaitc map,” *Chaos, Solitons and Fractals*, p. in press, 2007.

[18] K. Kelber and W. Schwarz, “General design rules for chaos-based encryption systems,” in *International Symposium on Nonlinear Theory and its applications*, 2005, pp. 465–467.

[19] L. Chuanmu and L. Hong, “A new image encryption scheme based on hyperchaotic sequences,” in *IEEE International Workshop on Anti-counterfeiting, Security, Identification*. IEEE, 2007, pp. 237–240.