



Article

Parallel Crossed Chaotic Encryption for Hyperspectral Images

Carlos Villaseñor, Eric F. Gutierrez-Frias, Nancy Arana-Daniel * , Alma Y. Alanis 
and Carlos Lopez-Franco

Centro Universitario de Ciencias Exactas e Ingenierías, Universidad de Guadalajara,
Blvd Marcelino García Barragán 1421, 44430 Guadalajara, México; cavp@outlook.com (C.V.);
eric.gfrias@academicos.udg.mx (E.F.G.-F.); almayalanis@gmail.com (A.Y.A.); clzfranco@gmail.com (C.L.-F.)

* Correspondence: nancyaranad@gmail.com; Tel.: +52-331-547-3877

Received: 29 June 2018; Accepted: 17 July 2018; Published: 20 July 2018



Featured Application: This work presents a time-efficient and parallel encryption algorithm that is suitable for encrypting a significant amount of data, and that could be used to encrypt Hyperspectral Images and Hyperspectral video in real-time for remote sensing, classification, object recognition, earth monitoring, security and medical applications.

Abstract: Hyperspectral images (HI) collect information from across the electromagnetic spectrum, and they are an essential tool for identifying materials, recognizing processes and finding objects. However, the information on an HI could be sensitive and must to be protected. Although there are many encryption schemes for images and raw data, there are not specific schemes for HI. In this paper, we introduce the idea of crossed chaotic systems and we present an ad hoc parallel crossed chaotic encryption algorithm for HI, in which we take advantage of the multidimensionality nature of the HI. Consequently, we obtain a faster encryption algorithm and with a higher entropy result than others state of the art chaotic schemes.

Keywords: chaotic encryption; hyperspectral images; parallel computing

1. Introduction

Nowadays Hyperspectral Images (HI) [1] are an essential tool for many research topics like Remote sensing [2], classification and object recognition [3] and Earth monitoring [4]. HI cameras collect information from across the electromagnetic spectrum retrieving more information than RGB cameras.

The HI is a three-dimensional arrange of numbers of size (n, m, l) , as is shown in Figure 1, where n is the numbers of rows, m the numbers of columns, and l the number of layers which every layer represents a range of light-waves.

In some HI applications, the information contained is sensitive, for example, in military or medical applications; then, it is essential to protect the information. There already exist many various algorithms for secure encrypting [5,6], like Advanced Encryption Standard (AES) [7–10] based on irreducible polynomials in Galois fields or the Rivest-Shamir-Adleman (RSA) algorithm [11] based on large prime number factorization. These algorithms offer a secure way to protect sensitive data, and they work with raw data, that is to say, they work at the binary level of data then they can deal with all kind of data structures like images, videos, and documents.

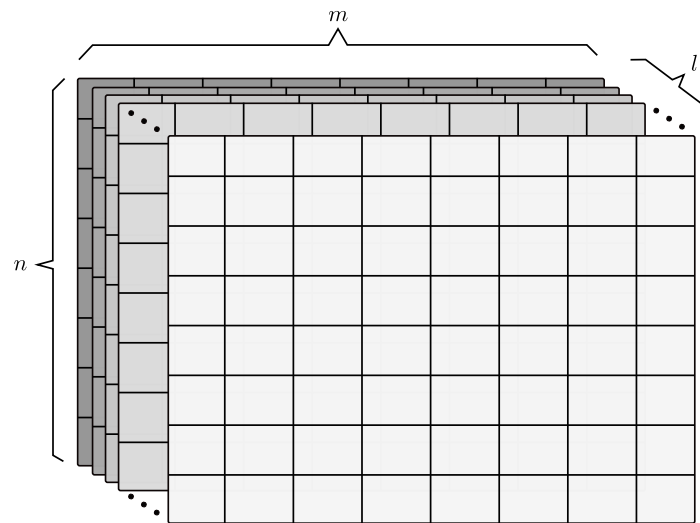


Figure 1. Hyperspectral Image.

However, algorithms like AES and RSA have a high computational cost; consecutively they are not suitable for encrypting a significant amount of data, or for real-time. For this reason, in recent years a new trend of encryption algorithms has been developed specifically for image and video [12]. In [12], we can find the following topics to consider in visual data encryption:

- **Security:** The required level of security of encrypting passwords or other structured data could differ than the one required for visual data. A more secure algorithm could impact with a high computational cost.
- **Speed:** A significant difference between visual data encryption and text-based encryption is that visual data is usually much larger. If we consider a time constraint or real-time execution requirements, the speed of encryption is an important issue.
- **Bitstream compliance:** Visual data could have a specific data format. Algorithms for raw data such as AES do not take data format into account and this could cause unexpected crashes in the image decoding.

Then, for image encryption algorithms it is highly desirable to obtain a good balance between security and speed. In the last decade, chaotic ciphers [13] have been very used algorithms for image encryption [14]. In [15], a comparison between chaotic and non-chaotic image encryption indicates that chaotic-based schemes are better because of chaos is nonlinear, deterministic and highly sensitive to initial conditions. This conclusion is based on a comparison of a correlation coefficient, information entropy analysis, compression friendliness, maximum derivation, uncertain derivation, avalanche effect, Number of Changing Pixel Rate (NPCR), Unified Average Changed Intensity (UACI) [16], and key space analysis. However, in nowadays chaotic image encryption schemes are specific for gray-scale images or RGB, and there is not an ad hoc encryption algorithm for HI. In the present paper, we propose a new chaotic encryption algorithm for HI which take advantage for designing a fast and high-entropy-valued algorithm. We also introduce the idea of crossed chaotic encryption (CCE), and we empirically show how CCE obtains better entropy results. Finally, we offer a comparison between serial and parallel implementations. The proposed algorithm obtain high-speed results in the parallel version, and high entropy compared with another state of the art algorithms.

The paper is structured as follows: In Section 2, we briefly review the basic properties of chaotic systems and chaotic encryption. In Section 3, we develop the idea of crossed chaotic encryption and the proposed scheme for HI. In Section 4, we show the results and comparison, and we also discuss the cryptanalytic features of the proposed algorithm. Finally, in Section 5 the conclusions are shown.

2. Chaotic Systems and Chaotic Encryption

In this section, we introduce some concepts of chaotic system and chaotic encryption.

2.1. Chaotic Systems

Chaotic systems are dynamical systems that exhibit the following features:

- **Deterministic:** There is no randomness involved in the system evolution, then if we know the initial condition and parameters, we will be able to predict the system.
- **Sensitive to initial conditions:** A chaotic system is exponentially sensitive to an initial condition, in other words, a small change in the initial condition provokes a big difference in the evolution of the system.
- **Aperiodic:** There is no periodicity in a chaotic system.
- **Bounded:** The state of a chaotic system is bounded, and it maintains chaotic inside this bounded limits.

The mentioned features make chaotic systems a suitable mathematical tool for encryption. Various chaotic systems have been used for encryption, such as the Lorenz system [17], Ikeda chaotic map [18] and others. Chaotic encryption has been used for electroencephalogram signal encryption [19], video encryption [20–22]. Chaotic systems, are also useful for designing bio-inspired optimization algorithms [23] or embed secret data with in the image [24].

2.2. Chaotic Encryption

We can distinguish between two types of chaotic encryption. The first one is based on the synchronization phenomena [25], where a chaotic system is combined with the on-line data stream and it is received with another chaotic system that synchronizes and enables us to filter the original data stream. Although this is a secure scheme, it only works for continuous data stream (e.g., airplanes telemetry), and not for static data because we could lose data during the system synchronization.

On the other hand, the second type where a chaotic signal is simulated and used to diffuse and confuse the plaintext information. In this paper, we focus on this second kind of encryption. Chaotic systems have been broadly used in image encryption, e.g., the logistic map is used in [26], 2D Arnolds Cat Map is compared to 3D logistic map for RGB image encryption [27], also 3D chaotic maps are used in general multimedia data [28].

Using different chaotic maps could increase the information entropy as is evidenced in [29]. In [14], a survey of image encryption is offered, and in [15] a comparison of different chaotic maps is shown.

2.3. Chaotic Image Encryption Performance

To measure the performance of the image chaotic encryption algorithms is common to use the information entropy defined in (1), where s_i is the intensity of the pixel i of the image, $P(s_i)$ is the probability of s_i intensity to appear. The $2^b - 1$ is the larger number represented in the data (255 for image intensity values), then the maximum theoretical value of entropy for the image of 256 intensity values is 8. Encrypted data that have a value of entropy close to the theoretical maximum is difficult to differentiate from random data, consequently it is secure against cypher-text-only attacks.

$$H(s) = - \sum_{i=0}^{2^b-1} P(s_i) \log_2[P(s_i)] \quad (1)$$

The idea of chaotic encryption is that using the chaotic behavior no algorithm could differentiate between an encrypted image and image full of random pixel values. A common technique in cryptanalysis is the differential attack, where we encrypt two different images with the same cipher. If the encrypted images are statistically different, then we could infer information about the cipher

secret key or parameters. In [16], two statistical measures are proposed to verify if cipher algorithm is weak against differential attack. The Number of Changing Pixel Rate (NPCR) is defined in Equation (3), where T is the total of pixels in the images and $D(i, j, k)$ is defined in (2), where I_1 and I_2 are two different images and c is a cipher algorithm.

$$D(i, j, k) = \begin{cases} 0 & \text{if } c(I_1(i, j, k)) = c(I_2(i, j, k)) \\ 1 & \text{if } c(I_1(i, j, k)) \neq c(I_2(i, j, k)) \end{cases} \quad (2)$$

$$NPCR(I_1, I_2, c) = \sum_{i,j,k} \frac{D(i, j, k)}{T} \times 100\% \quad (3)$$

The Unified Average Changed Intensity (UACI) is defined in (4), where F is the maximum intensity value allowed. To ensure that the encrypted image is not differentiable of a image full of random pixel values, the expected values of NPCR and UACI are $NPCR_e = 99.6094\%$ and $UACI_e = 33.4634\%$.

$$UACI(I_1, I_2, c) = \sum_{i,j,k} \frac{|c(I_1(i, j, k)) - c(I_2(i, j, k))|}{F \cdot T} \times 100\% \quad (4)$$

2.4. Piecewise Linear Chaotic Map

The algorithm proposed in this paper, is based on the Piecewise Linear Chaotic Map (PLCM), but it can be implemented with any other chaotic map. The PLCM is defined in (5), where x_n is the state of the system and q is a parameter. The PLCM shows a chaotic behaviour when the parameter $q \in (0, 0.5)$ and the state x_n is bounded inside the interval $(0, 1)$.

$$x_{n+1} = c(x_n, q) = \begin{cases} \frac{x_n}{q} & \text{if } x \in [0, q) \\ \frac{x_n - q}{0.5 - q} & \text{if } x \in [q, 0.5) \\ c(1 - x_n, q) & \text{if } x \in [0.5, 1) \end{cases} \quad (5)$$

The authors in [30] propose an improved version of the PLCM, called Modified Piecewise Chaotic Map (MPLCM). They report an information entropy of 7.9972–7.9976. This result overcomes the 7.8472–7.9413 reported in [29]. The MPLCM is defined in (6) and a simulation is shown in Figure 2.

$$x_{n+1} = c(x_n, q) = \frac{x_n - \lfloor \frac{x_n}{q} \rfloor q}{q} \quad (6)$$

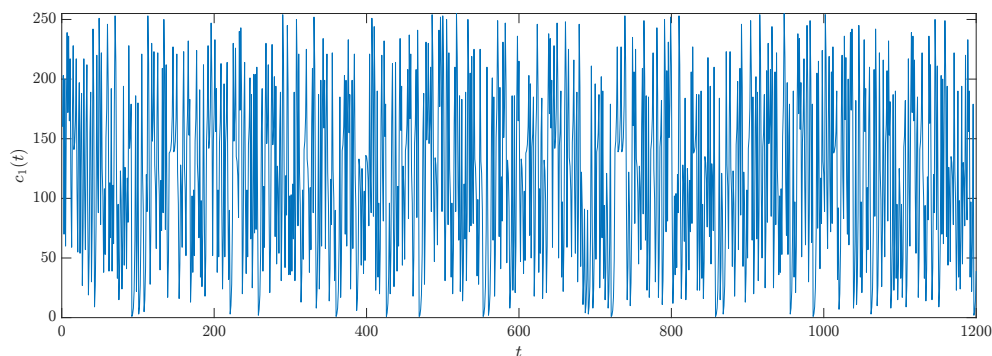


Figure 2. MPLCM simulation.

3. Encryption for Hyperspectral Images

One of the main disadvantages of using chaotic encryption is that we have to simulate the chaotic system until we have the same amount of information than the one to be encrypted. For this reason,

the chaotic systems are commonly used as a stream cipher. To overcome this problem, we propose to use a crossed scheme, where a p -dimensional chaotic signal is generated through the XOR of 1-dimensional systems, this is denoted in (7).

$$C_p(i_1, i_2, \dots, i_p) = c_1(i_1) \oplus c_1(i_2) \oplus \dots \oplus c_p(i_p) \quad (7)$$

In Figure 3, we present how two chaotic systems can generate a chaotic two-dimensional signal.

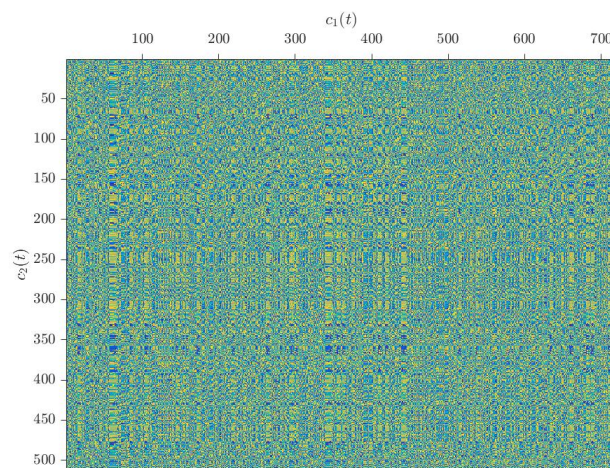


Figure 3. 2D Crossed Chaotic Signal.

Therefore using crossed chaotic signals we can generate a multi-dimensional chaotic signal without simulating a chaotic system for the dimension of the data to be encrypted. Based in crossed chaotic signal, we propose the following encryption scheme in Figure 4.

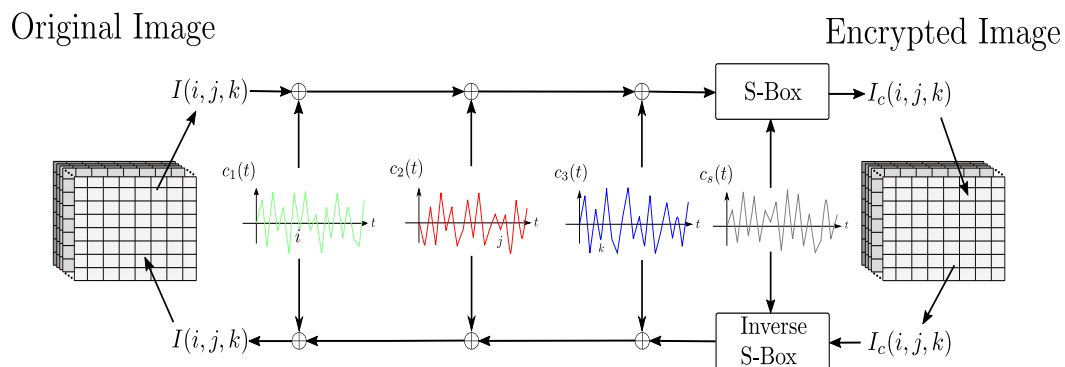


Figure 4. Chaotic Encryption Scheme.

We propose to use four chaotic systems. The first three systems form a three-dimensional crossed chaotic signal, and they are used to introduce diffusion in the result. They are simulated for $\max(n, m, l)$ iterations. The fourth chaotic system is used to creating a Substitution Box (S-Box) [31], we use the generation algorithm proposed in [32]. S-boxes are used for introducing confusion in the encryption and is a common technique applied in AES and other block ciphers [33].

It is important to note that the proposed scheme is a transformation that is made pixel by pixel, this is because we are looking for a high parallelizable algorithm. Then the encryption of the pixel

(i, j, k) is applied with (8) and the decrypted pixel is recover with (9). In the Algorithm 1, we present the parallel version of this algorithm.

$$I_c(i, j, k) = S_{box} [c_3(k) \oplus c_2(j) \oplus c_1(i) \oplus I(i, j, k)] \quad (8)$$

$$I(i, j, k) = c_1(i) \oplus c_2(j) \oplus c_3(k) \oplus S_{box}^{-1} [I_c(i, j, k)] \quad (9)$$

Algorithm 1: Parallel Crossed Chaotic Encryption.

Data: Hyperspectral Image I

Result: Encrypted Image I_c

Simulate all chaotic systems $\{c_1, c_2, c_3, c_s\}$ in parallel for $\max(n, m, l)$ iterations;

Generate S-box with c_s ;

Upload I to GPU memory;

In parallel apply $I_c(i, j, k) = S_{box} [c_3(k) \oplus c_2(j) \oplus c_1(i) \oplus I(i, j, k)]$;

Download I_c to CPU memory;

4. Results

To demonstrate the performance of the proposed algorithm, we offer the following results. These experiments were carried out in an Intel Xeon[®] E31225 3.10 GHz, with a 16 GB of RAM and a GTX 1050Ti. The algorithm was implemented in Matlab[®] programming language and with GPU computing support for Nvidia CUDA[®]. The GTX 1050Ti have 768 cores and 4 GB of memory.

In Figure 5, we present an encryption over “San Francisco with Polarizing filter” HI, from the Scene Database 4 of ImageVal Consulting[®] (Database from <http://www.imageval.com>). The image size is $702 \times 1000 \times 148$ (we show in Figure 5 the layer 50) and the light-wave is 415–915 nm. The entropy of the original image is 6.1057 and the encrypted entropy is 7.99997, very close to the theoretical maximum entropy.

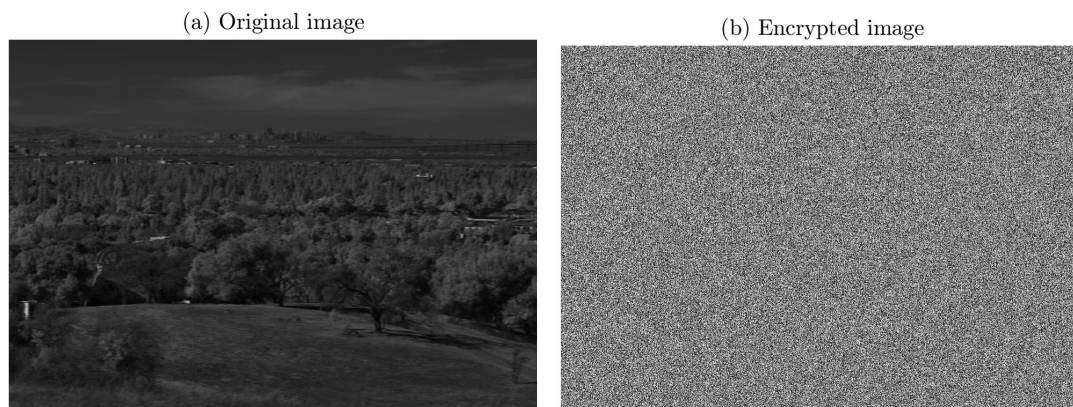


Figure 5. Experiment 1. Original and encrypted images.

We also show in Figure 6, the normalized hyperhistogram where we calculate the histogram of every layer. Please note that the encrypted image has a hyperhistogram approximately uniform.

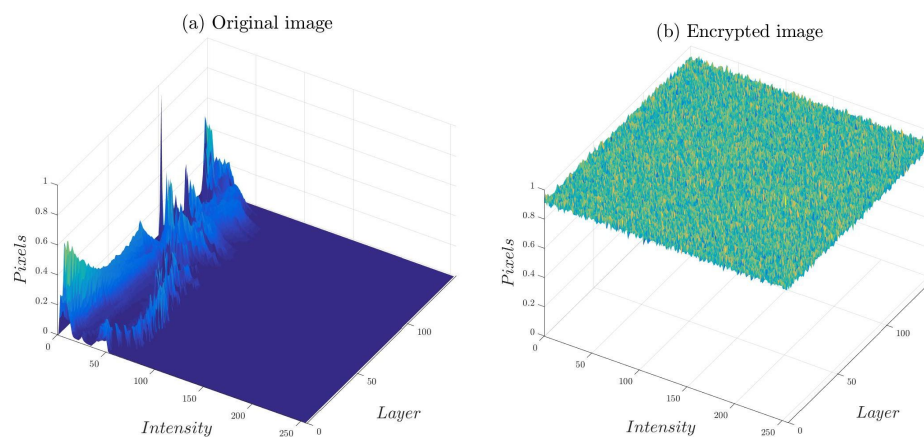


Figure 6. Experiment 1. Hyperhistogram of original and encrypted images.

In this way, to show the time advantage of using an ad hoc encryption technique for HI, consider the data set shown in Table 1, where the sizes of 24 HI of women and men faces (this data set is taken from Hyperspectral High-Resolution Faces of the Scene Database of ImageVal Consulting® (Taken from <http://www.imageval.com/scene-database/>)). The dataset consists of 12 portraits of women and 12 of men with a light-wave spectrum of 415–915 nm. We show the file size and the image size.

Table 1. HI face images dataset.

Female Dataset					Male Dataset				
Name	Size (MB)	Dimensions			Name	Size (MB)	Dimensions		
		<i>n</i>	<i>m</i>	<i>l</i>			<i>n</i>	<i>m</i>	<i>l</i>
Female01	922	1403	975	29	Male01	993	1349	965	41
Female02	820	1169	912	42	Male02	974	1294	969	43
Female03	993	1346	935	46	Male03	949	1337	948	39
Female04	906	1279	912	43	Male04	927	1322	981	35
Female05	802	1260	904	33	Male05	851	1379	969	24
Female06	651	1237	855	21	Male06	894	1317	1066	24
Female07	1014	1368	942	45	Male07	986	1447	1044	26
Female08	883	1322	955	33	Male08	1013	1423	1059	30
Female09	952	1323	1043	31	Male09	920	1366	938	35
Female10	763	1197	970	27	Male10	1085	1271	1038	50
Female11	867	1213	929	42	Male11	1105	1414	975	47
Female12	771	1214	914	32	Male12	937	1317	981	36

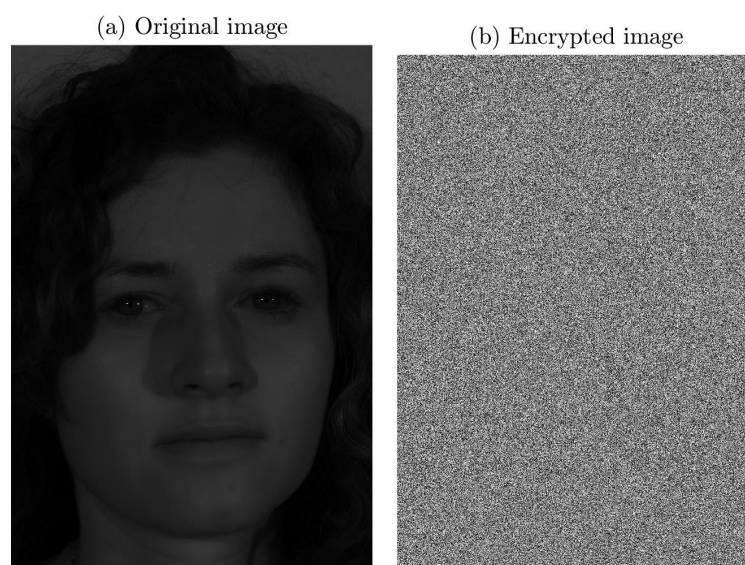
In Tables 2 and 3, we present the results of the encryption of the female and male faces datasets, respectively. We show the serial time and the parallel time. In the parallel time, we also include the upload to GPU and the download to CPU times, such time is achieved thanks to the high parallelism of the scheme. We also show the original and encrypted entropy. In Figure 7, we show an example of the Female06 image with the respective hyperhistograms. In the same way, and Figure 8 shows an example of the Male03 image with the respective hyperhistograms.

Table 2. Female dataset encryption results.

Name	Serial Time (s)	Parallel Time(s)				Entropy	
		Upload	Encrypt	Download	Total	Original	Encrypted
Female01	12.4671	0.0194	0.003338	0.0231	0.045838	7.6478	7.99995
Female02	14.5577	0.0220	0.003502	0.0259	0.051482	6.9685	7.99994
Female03	18.0801	0.0289	0.004160	0.0323	0.065360	7.7217	7.99994
Female04	15.3995	0.0249	0.003745	0.0290	0.057645	7.4850	7.99994
Female05	11.4269	0.0188	0.003177	0.0225	0.044477	6.9084	7.99994
Female06	6.6332	0.0129	0.002135	0.0139	0.028935	7.5043	7.99996
Female07	17.8849	0.0286	0.004158	0.0332	0.065958	7.7350	7.99997
Female08	12.8754	0.0208	0.003407	0.0249	0.049107	7.5038	7.99994
Female09	13.5488	0.0230	0.005120	0.0420	0.070120	6.0217	7.99995
Female10	10.5763	0.0164	0.003324	0.0186	0.038324	7.0142	7.99996
Female11	14.7164	0.0215	0.003804	0.0243	0.049604	6.9170	7.99994
Female12	11.4762	0.0145	0.002545	0.0194	0.036445	7.2636	7.99994

Table 3. Male data set encryption results.

Name	Serial Time (s)	Parallel Time(s)				Entropy	
		Upload	Encrypt	Download	Total	Original	Encrypted
Male01	16.6417	0.0253	0.00353	0.0304	0.05923	7.6170	7.99994
Male02	16.9902	0.0249	0.00356	0.0301	0.05856	7.2491	7.99994
Male03	15.0768	0.0243	0.00346	0.0298	0.05756	7.4629	7.99994
Male04	14.8045	0.0239	0.00351	0.0301	0.05751	7.4662	7.99995
Male05	10.4175	0.0186	0.00295	0.0275	0.04905	7.3869	7.99995
Male06	9.8852	0.0187	0.00334	0.0256	0.04764	7.7191	7.99996
Male07	11.8605	0.0225	0.00421	0.0261	0.05281	7.0507	7.99995
Male08	14.7449	0.0246	0.00394	0.0311	0.05964	7.2739	7.99995
Male09	13.2484	0.0225	0.00284	0.0294	0.05474	7.2322	7.99994
Male10	22.14	0.0351	0.00353	0.0395	0.07813	7.4603	7.99996
Male11	20.9537	0.0346	0.00467	0.0481	0.08737	7.3924	7.99995
Male12	13.939	0.0253	0.00347	0.0331	0.06187	7.3524	7.99995

**Figure 7.** Cont.

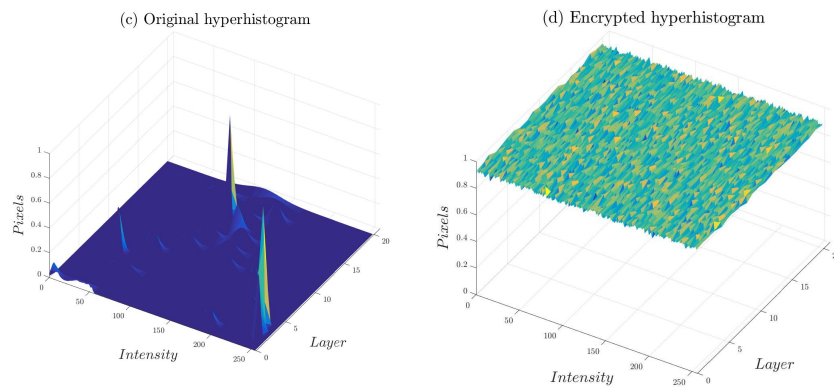


Figure 7. Original and encrypted image (layer one) of Female06 HI.

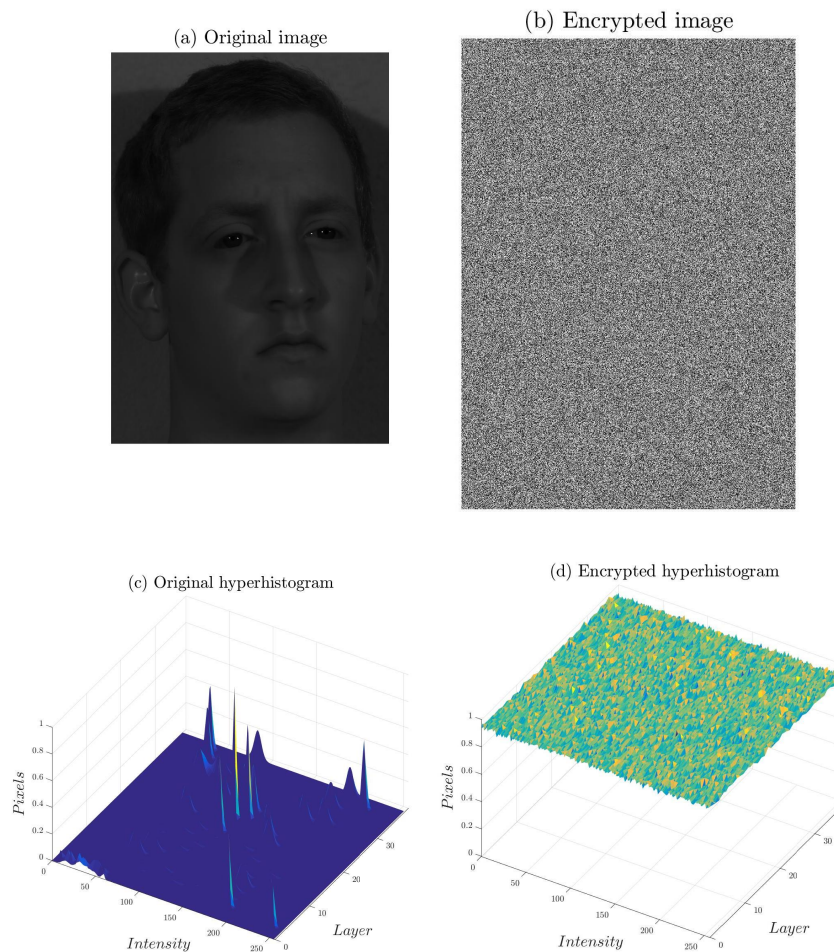


Figure 8. Original and encrypted image (layer one) of Male03 HI.

Please note that the time in parallel is minimal compared with the serial time, this is due to the high parallelism in the cipher scheme. Furthermore, the information entropy is very close to the theoretical maximum entropy. This results overcome the results reported in [29,30], for gray-scale and RGB images.

The key of the proposed cipher is the parameters and the initial conditions of the chaotic systems, this can be improved with key establishment protocols [34] and chaotic-based hash functions [35].

In this manner, to test the strength against cryptanalytic differential attacks [36], we apply the NPCR, and UACI tests [16]. As we need two images of the same size, we trim the Female09 image to the Female10 image size. Then, we encrypt the two images with the same cipher and the same key and run NPCR and UACI test with the results displayed in Table 4. Please note that the result values approximate the expected values of a random image, then we can claim that the cipher is protected against differential attacks.

Table 4. NPCR and UACI analysis.

Input Images	NPCR	UACI
Female09 and Female10	99.6186	33.4595

5. Conclusions

In this paper, we present a new chaotic encryption algorithm specifically designed for hyperspectral images. We also present the new idea of crossed chaotic signals that solve the problem of simulating a system for many iterations, using a family of 1-dimensional chaotic maps instead. The proposed algorithm is fast in its parallel version, and it achieves high information entropy (very close to the theoretical maximum) and an approximately uniform hyperhistogram. High entropy and uniform histogram make it safe against Ciphertext-only attacks and their statistical tools. Furthermore, we applied the NPCR and the UACI tests to the cipher, and we show strength against cryptanalytic differential attacks.

Author Contributions: Conceptualization, C.V. and N.A.-D.; Formal analysis, C.V. and E.F.G.-F.; Funding acquisition, A.Y.A. and C.L.-F.; Investigation, C.V., N.A.-D.; Methodology, C.V.; Project administration, N.A.-D.; Software, C.V.; Supervision, N.A.-D. and C.L.-F.; Validation, E.F.G.-F.; Writing—original draft, C.V.; Writing—review and editing, N.A.-D. and A.Y.A.

Funding: This work has been supported by CONACYT Mexico, through Projects CB256769 and CB258068 (“Project supported by Fondo Sectorial de Investigación para la Educación”).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chang, C.I. *Hyperspectral Imaging: Techniques for Spectral Detection and Classification*; Springer Science & Business Media: Heidelberg/Berlin, Germany, 2003; Volume 1.
2. Melgani, F.; Bruzzone, L. Classification of hyperspectral remote sensing images with support vector machines. *IEEE Trans. Geosci. Remote Sens.* **2004**, *42*, 1778–1790. [[CrossRef](#)]
3. Camps-Valls, G.; Bruzzone, L. Kernel-based methods for hyperspectral image classification. *IEEE Trans. Geosci. Remote Sens.* **2005**, *43*, 1351–1362. [[CrossRef](#)]
4. Camps-Valls, G.; Tuia, D.; Bruzzone, L.; Benediktsson, J.A. Advances in hyperspectral image classification: Earth monitoring with statistical learning methods. *IEEE Signal Process. Mag.* **2014**, *31*, 45–54. [[CrossRef](#)]
5. Paar, C.; Pelzl, J. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer Science & Business Media: Heidelberg/Berlin, Germany, 2009.
6. Buchmann, J. *Introduction to Cryptography*; Springer Science & Business Media: Heidelberg/Berlin, Germany, 2013.
7. Thulasimani, L.; Madheswaran, M. A single chip design and implementation of aes-128/192/256 encryption algorithms. *Int. J. Eng. Sci. Technol.* **2010**, *2*, 1052–1059.
8. Moh’d, A.; Jararweh, Y.; Tawalbeh, L. AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation. In Proceedings of the 2011 7th International Conference on Information Assurance and Security (IAS), Melaka, Malaysia, 5–8 December 2011; pp. 292–297.
9. Guo, G.L.; Qian, Q.; Zhang, R. Different implementations of aes cryptographic algorithm. In Proceedings of the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, New York, NY, USA, 24–26 August 2015; pp. 1848–1853.

10. Zhu, Y.; Zhang, H.; Bao, Y. Study of the AES realization method on the reconfigurable hardware. In Proceedings of the 2013 International Conference on Computer Sciences and Applications, Wuhan, China, 14–15 December 2013; pp. 72–76.
11. Coutinho, S.C. *The Mathematics of Ciphers: Number Theory and RSA Cryptography*; AK Peters/CRC Press: Boca Raton, FL, USA, 1999.
12. Uhl, A.; Pommer, A. *Image and Video Encryption: From Digital Rights Management to Secured Personal Communication*; Springer Science & Business Media: Heidelberg/Berlin, Germany, 2004; Volume 15.
13. Kocarev, L.; Lian, S. *Chaos-Based Cryptography: Theory, Algorithms and Applications*; Springer: Heidelberg/Berlin, Germany, 2011; Volume 354.
14. Sankpal, P.R.; Vijaya, P. Image encryption using chaotic maps: A survey. In Proceedings of the 2014 Fifth International Conference on Signal and Image Processing, Bangalore, India, 8–10 January 2014; pp. 102–107.
15. Bansal, R.; Chawla, R.; Gupta, S. A comparison of image encryption techniques based on chaotic maps. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 933–938.
16. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. *J. Sel. Areas Telecommun. (JSAT)* **2011**, *1*, 31–38.
17. Zhang, L.; Zhang, Y. Research on lorenz chaotic stream cipher. In Proceedings of the 2005 IEEE International Workshop on VLSI Design and Video Technology, Suzhou, China, 28–30 May 2005; pp. 431–434.
18. Jia, X. Image Encryption using the Ikeda map. In Proceedings of the 2010 International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Kuala Lumpur, Malaysia, 22–23 June 2010; pp. 455–458.
19. Lin, C.F.; Wang, B.S. 2D Chaos-Based Visual Encryption Mechanism in EEG Signals. In Proceedings of the 2010 International Symposium on Parallel and Distributed Processing with Applications (ISPA), Taipei, Taiwan, 6–9 September 2010; pp. 470–473.
20. Lian, S.; Sun, J.; Wang, Z.; Dai, Y. A fast video encryption scheme based-on chaos. In Proceedings of the Control, Automation, Robotics and Vision Conference, Kunming, China, 6–9 December 2004; Volume 1, pp. 126–131.
21. Shang, F.; Sun, K.; Cai, Y. An efficient MPEG video encryption scheme based on chaotic cipher. In Proceedings of the Image and Signal Processing, Sanya, China, 27–30 May 2008; Volume 3, pp. 12–16.
22. Su, Z.; Lian, S.; Zhang, G.; Jiang, J. Chaos-based video encryption algorithms. In *Chaos-Based Cryptography*; Springer: Heidelberg/Berlin, Germany, 2011; pp. 205–226.
23. Mhatre, R.M.; Bhardwaj, D. Classifying Iris Image Based on Feature Extraction and Encryption Using Bio-Chaotic Algorithm (BCA). In Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 12–14 December 2015; pp. 1068–1073.
24. Muhammad, N.; Bibi, N.; Mahmood, Z.; Akram, T.; Naqvi, S.R. Reversible integer wavelet transform for blind image hiding method. *PLoS ONE* **2017**, *12*, e0176979. [[CrossRef](#)] [[PubMed](#)]
25. Parlitz, U.; Junge, L. Synchronization of chaotic systems. In Proceedings of the Control Conference (ECC), Karlsruhe, Germany, 31 August–3 September 1999; pp. 4637–4642.
26. Fu, C.; Zhang, Z.C.; Chen, Y.; Wang, X.W. *An Improved Chaos-Based Image Encryption Scheme*; Springer: Heidelberg/Berlin, Germany, 2007; pp. 575–582.
27. Khade, P.N.; Narnaware, M. 3D chaotic functions for image encryption. *IJCSI Int. J. Comput. Sci. Issues* **2012**, *9*, 323–328.
28. Hossain, M.B.; Rahman, M.T.; Rahman, A.S.; Islam, S. A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. In Proceedings of the 2014 International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, 23–24 May 2014; pp. 1–6.
29. Sathishkumar, G.; Bagan, K.B.; Sriraam, N. Image encryption based on diffusion and multiple chaotic maps. *arXiv* **2011** arXiv:1103.3792.
30. Hu, Y.; Zhu, C.; Wang, Z. An improved piecewise linear chaotic map based image encryption algorithm. *Sci. World J.* **2014**, *2014*. [[CrossRef](#)] [[PubMed](#)]
31. Wolkerstorfer, J.; Oswald, E.; Lamberger, M. *An ASIC Implementation of the AES SBoxes*; Springer: Heidelberg/Berlin, Germany, 2002; pp. 67–78.
32. Mroczkowski, P. Generating Pseudorandom S-Boxes-a Method of Improving the Security of Cryptosystems Based on Block Ciphers. *J. Telecommun. Inf. Technol.* **2009**, *2*, 74–79.

33. Kazmi, S.; Ikram, N. Chaos based key expansion function for block ciphers. *Multimed. Tools Appl.* **2013**, *66*, 267–281. [[CrossRef](#)]
34. Das, M.L.; Narasimhan, V.L. A simple and secure authentication and key establishment protocol. In Proceedings of the Emerging Trends in Engineering and Technology, Maharashtra, India, 16–18 July 2008; pp. 844–849.
35. Gao, L.; Wang, X.; Zhang, W. Chaotic hash function based on Tandem-DM construction. In Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Changsha, China, 16–18 November 2011; pp. 1745–1749.
36. Solak, E. Cryptanalysis of chaotic ciphers. In *Chaos-Based Cryptography*; Springer: Heidelberg/Berlin, Germany, 2011; pp. 227–256.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).