International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3727

E-ISSN : 2454-6135

Volume.7, No. 7
July -2021

Subject Review: Image Encryption Techniques based on Chaotic Systems

Donia Fadhil Chalob, Zynab M. Jasim, Zainab Mohammed Essa, and **Ziad M. Abood***

Collage of Education

Mustansiyiah University

Iraq

ABSTRACT

The interchange of information over the internet and networks has grown fast. The Digital images occupy an important role in multimedia communications. Images are utilized in a variety of discipline, including biometric authentication, military, medical science; hence, their security become a major concern. The best solution for securing the data (in any form) is encryption. The recent encryption trend is chaos-based encryption. Image encryption approaches based on chaos have essential merits l. This paper surveys various aspects and approaches of chaos maps image encryption like PWLCM (piecewise linear chaotic map), logistic map, skew tent map. Considering security measurements like correlation analysis and keyspace when comparing image encryption techniques that use different chaotic maps.

Keywords: Chaos Theory, Image Encryption, DNA, Security.

1. INTRODUCTION

During transmission and storage, image encryption is utilized to protect information in an image from unapproved access. [1]

1.1 What is Image Encryption?

Image encryption can be accomplished via changing pixel position in addition to alter the pixels contents , resulting in a full alteration in the image's content. Various methods like cryptography, compression, watermarking and steganography can be applied for image encryption. Chaotic cryptography is the techniques where chaos-based encryption can be used to encrypt images. [1]

1.2 What is Chaotic Systems?

The application of mathematical chaos theory for encryption is known as chaotic cryptography. Chaotic encryption utilizes chaotic maps to create diffusion and confusion. The properties of chaotic approach are ideal for image cryptography. Sensitivity towards initial conditions is a characteristic of chaos where a tiny alteration of initial conditions consequences a big change in the system, to decrypt an image, for example , a precise initial condition is required. Various chaos systms are utilized in cryptography. A chaotic system is a result of a function which demonstrates chaos. To generate random numbers, chaos maps are employed. Logistic map, Tent map, Baker's Map, Renyi map is examples of chaos maps. The sequence of numbers that generated keys in image cryptography is generated using chaos systems. Image encryption and decryption require chaotic systems to obtain specific properties, one of which is sensitive towards initial condition, Figure 1(a) demonstrates the diagram of logistic map over time vs the value derived from logistic map for two distinct initial conditions. The red line represents the diagram of the logistic map at x0 = 0.2, while a green line represents the diagram of a logistic map at x0 = 0.200001. The plot of the variance between values for two initial conditions of the logistic map, x0=0.2 and x0=0.200001, is shown in Figure1(b). One can notice that the variance of values created by logistic map is big, while the variance between the two initial condition is tiny. Sensitive to initial condition is the name given to this characteristic. The property of sensitive to initial condition in chaos system could be utilized in image cryptography. Chaos system is utilized to produce pseudorandom number, where the numbers produced via the chaos map have the features of chaotic maps are identical to those of random number; yet they aren't random because they can be regenerated by passing the identical initial conditions. Chaotic system shows a characteristic identified as ergodicity, a system is called ergodicity when it is irreducibility. The features of chaos systems mentioned above can be utilized to effectively encrypt and decrypt images. [2-3]

This paper reviews various methods to show the chaos map for image cryptography. The remain of the paper is set as following: Section (2) provides a survey of the literature on image cryptography via chaos map. Section 3 compares image cryptography via chaos maps among other methods. Last, Section 4 gives conclusion.

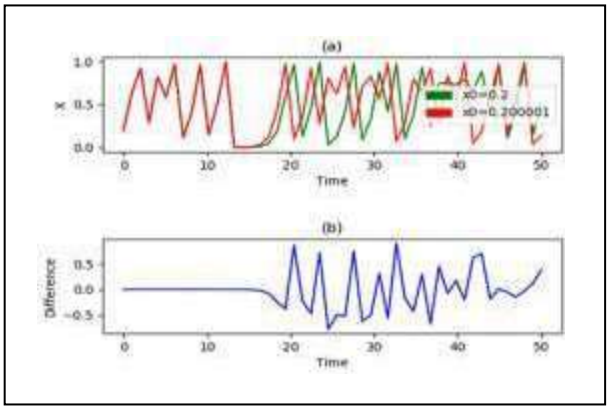

Figure 1: Logistic Map Plot (a) Two Initial Conditions of Logistic Map (b) Variance between Values for Two Initial Conditions of Logistic Map. [1]

2. LITERATURE SURVEY

Numerous image cryptography methods based on chaos theory have been investigated during last decade. Some of these studies are discussed in this section.

Wang et al. [4] proposed an image cryptography depend on DNA (Deoxyribonucleic acid) sequence processes based on chaos map. First, bitwise XOR process is executed on the original image pixels by random sequences formed via the spatiotemporal chaotic map, named as CML (Coupled Map Lattice). The CML system's starting conditions are produced using an Extended Hamming distance; the initial values for encryption are dependent on the plaintext image. Second, encoding the permuted image with a DNA encoding rule yields a DNA matrix. Next, apply different CML system initial values on DNA array as well as the preceding initial conditions, causing the outcome of the encryption to be highly dependent on each pixel of original image. Third, shuffling each row and column of DNA matrix, the shuffled DNA array is scrambles once more. Finally, the encrypted image is acquired after a DNA decoding rule to decode the shuffled matrix DNA.

Lu Xu et al. [5] suggest a new chaotic image cryptography scheme, a block bu block image scrambling approach and a dynamic index built diffusing system. The plain image is divided into two blocks of equal size first via moving it vertically or horizontally. If the row number is odd and the row to split. Then, at random, add a row. Likewise, if the number of columns in the table is odd and the column to divide, add a column at random. The chaotic array is utilized to produce X coordinate, Y coordinate and swap control table. The swap location of processing pixel is found by examining X and Y coordinate table. The swap control table controls whether a pixel in one block or another is swapped. At last, for diffusing images, the dynamic index technique is good that have been scrambled. The indices are used to locate specific locations in encrypted and unencrypted pixel sequences, correspondingly. The processing pixel is encrypted using two pixels in the places. Double image scrambling can also benefit from the suggested scrambling strategy. This approach employs logistic map, which, despite the disadvantage of periodic windows, is simple and quick to implement. Keep the parameters close to 4 to achieve a decent chaotic sequence.

Zahmoul et al. [6] proposed a chaotic image cryptosystem depended on Beta function which is a basic mathematical tool. The vast domain of bifurcation parameters, robust chaotic performance, enhanced pseudorandom chaotic sequences and high quantity of parameters all contribute to the power of these maps. In order to produce chaotic pseudorandom sequences, numerous combinations of these maps in the suggested encryption algorithm are used. Permutation, Diffusion and Substitution are the three phases of the proposed approach. To muddle the relationship between the encrypted and plain images by scrambling the position of image pixels, multiple pseudorandom sequences were generated.

Zhou et al. [7] organize a chaotic system that combines two known one dimensional chaotic maps, seed maps and a new image cryptography method. When applied on an identical plain image with the same set of security keys, this approach produces an entirely different cipher image each time. The suggested technique employs a four-round cipher structure, every round involving five phases. First, in the plain image, putting a random pixel at the start of each row. After that, every row is separated into a one dimensional array and each 1-D matrix is subjected to a replacement operation to change the data values. Based on their row locations in the plain image, merge the entire 1-D matrices into a 2-D data matrix, and counterclockwise rotates the 2-D matrix 90 degrees. Repeat these procedures four times to get the final cipherS image.

Chai et al. [8] suggested image encryption technique depend on DNA (deoxyribonucleic acid) series processes, chaos map and SHA-256 Hash function. The plain image is first encoded to a DNA matrix, after that it is subjected to a new wave-based permutation technique.

Chiou et al. [9] used the three-dimensional chaos logistic map to cipher colour image. At first, the 3-D logistic map is adapted to produce key stream and following a sequences of transformations. By running XOR and shifting operations for a few rounds, the sequences build a new pseudorandom sequence that distributes uniformly in the value space and covers the plaintext to form the cipher image.

AL-Hashemy and Mehdi [10] used a novel 3D chaotic system depend on magic square, the new system generates a random key to cipher colour images. This chaotic system generates an image-sized number of chaos keys, which are next set into an array and split into non overlapping submatrices. To construct a new set of matrices, the plain image is split into sub-images, each of which is multiplied by a magic array. The resultant two sets of matrices are subjected to the XOR technique to generate the cipher.

Rasul Enayatifar et al. [11] suggest a new technique depend on a deoxyribonucleic acid (DNA), a Tinkerbell chaotic map hybrid model and CA (cellular automata). DNA rules, DNA sequence XOR operation and CA rule are all used at the same time to encrypt the plain image pixels. A two-dimensional Tinkerbell chaotic map is used to specify the rule number in DNA sequence and CA.

Kamlesh Gupta and Sanjay Silakari [12] suggested to execute confusion and diffusion operations on color images using a 3-D standard and 3-D Cat map image cryptosystem scheme. The plain image is split into three levels, the red band is rotated vertically, the green band is rotated horizontally and the blue band remaining unchanged. Then, each band is permuted using a 3-D cat map and 3-D standard map. Finally, XOR is utilized to combine the encryption operations.

Boriga et al. [13] suggested a symmetric stream image cryptography algorithm, via used three 2D chaotic maps a confusion step, where the pixels are scrambled via a random scrambling produced via a new efficient scheme and diffusion step, where the pixels' values are changed via a new XOR-technique.

Alireza Arab et al. [14] suggested a new image cryptosystem depend on chaos sequence and modified-AES algorithm. Arnold chaotic sequence is used to produce the encryption key in this technique. The plain image is encrypted with a modified AES method and round keys produced by the chaos system. The Arnold chaos system is utilized to generate the encryption key , the image is ciphered using the proposed method, namely modified AES algorithm. The variance between the original and modified AES is that the operation block in modified method is the exact size as the image and the substitution and column integration operation in this method are exchanged via new methods. Two modifications to the original AES technique are included in these terms: The first change is that the suggested propagation processes are replaced with permutable operations, where the second change is that the linear transform method is replaced with the column integration operation. The plain image is then encrypted with the 10 round keys obtained by the chaotic system with a modified AES algorithm.

Rafik Hamza and Faiza Titouna [15] proposed an image cryptosystem depend on 2D Zaslavsky map using confusion and diffusion structure. There are two parts in the proposed technique. The proposed cryptosystem's initial phase generates encryption keys using the 2D Zaslavsky chaotic map. These keys are used in the second phase to confuse and diffuse the pixels of the original image via confusion-diffusion operations. Multiplication of matrices over a finite field $Gf(2^8)$, the proposed algorithm uses the matrix K with its invertible L to acquire a good level of sensitivity to the plain image.

Kaixin Jiao et al. [16] offered an image cryptosystem depend on generalize Arnold map and the RSA algorithm (Rivest–Shamir–Adleman). The RSA asymmetric technique is utilized to produce the parameters of the generalize Arnold map, the key stream is created continuously. The image is masked via XOR diffusion to modify the pixel values distribution. Second, mask the image pixel once more, the image's rows and columns are cyclically scrambled. To achieve third layer image content concealing, the additive mode diffusion operation is used. The whole confusion and diffusion processes are repeated again to gain the finishing encrypted image.

Manjit Kaur and Vijay Kumaran [17] suggested an image cryptosystem using genetic algorithm, beta chaos map and nonsubsampled contourlet transformation. The input image is first divided into subbands via the nonsubsampled contourlet transform. For encrypting subband coefficients, the beta chaos map is utilized to obtain a pseudorandom key. Though, it involves particular parameters to cipher these coefficients. The objective of a genetic algorithm's multiobjective fitness function is to find the best beta chaos map parameter. The cipher image is acquired via the reverse of nonsubsampled contourlet transformation.

Choi et al. [18] suggested medical image cryptosystem depend on Combined Cellular Automata (CoCA). CoCA is made up of a 3D generalized chaotic map, a non-linear CA and a 90/150 linear length CA. There are two phases of this encryption algorithm. The initial phase uses two CoCAs to differ the values of pixel of a particular image. The second step involves shuffling of every pixel in the encrypted image via a 3D generalize chaos cat map, which modify the place of pixels in 2D space both in horizontal and vertical way, as well as in three colored planes in the color plane simultaneously.

Hao Li et al. [19] suggested the 32-bit PL PWLCM&LM, a positive integer random series producer, two 32-bit PL PWLCMs and one 32-bit logistic map are running in parallel in this system. The scrambling technique by four pixels as a scrambling unit is adopted in this proposed image encryption and the diffusion operation is depended on the rows and columns. This study proposed a 32-bit PL PWLCM&LM integer randomness series generation system to achieve an appropriate precision level of random numbers and overcome the processing of the floating-point number generated from a chaotic system.

The scheme's operations can all be carried out in the integer domain. The system is connected in parallel. A two-round PDN model is utilized in the system. One round of four pixel unit confusion and two rounds of row and column diffusion are included in each round of encryption. Merely a pseudorandom series of 25% of image size is required to accomplish one round of cipherment.

Yong Zhang and Yingjun Tang [20] presented a symmetric image cryptosystm depend on PWLCM (PieceWise Linear Chaotic Map). In this algorithm, both encryption and decryption operations are identical. They're both made up of the same precise methods for generating secret key streams. The PWLCM is utilized to generate pseudorandom sequences, Plaintext shuffling once, diffusion twice and 180-degree array rotation 4 times. The algorithm's secret key is (64d) characters long, where d is a positive integer.

Heba G. Mohamed et al. [21] employed a confusion method depend on a 4D hybrid chaotic map for color image encryption. First, divide each plane of images into n-clusters; next scramble the entire image with a global scrambler. Finally, apply intrapixel scrambling to each cluster, resulting in a cipher image with exceedingly disordered pixels. The human mitochondrial genome mtDNA is then utilized to disperse the earlier pixels confusion. Two main phases involves; the image pixels are shuffled depend on the resulting hyperchaotic sequence in the first step, the confusion phase. The location of pixels are scattered over the entire image, but their significance remains the same to increase unpredictability encryption efficiency. Hence, the primary and control parameters of the chaos systems are utilized as the concealed key. The second step, the diffusion step, the Exclusive OR (XOR) method is utilized to diffuse pixels with the decimal converted values of the mtDNA sequence.

Rui Wang et al. [22] suggested an image cryptosystem depend on chaos map and Josephus problem. The encryption operation utilizes the classic confusion–diffusion method. By refining the chaotic shift transform approach, the double chaotic cycle shift technique is presented in permutation phase. The diffusion phase involves preserving the Josephus sequence variety and expanding the Josephus problem notion through the use of chaotic maps. Then, the image is split into subblocks and choose one at random as stated by Josephus sequence. The image pixels can be reformed by execution modular addition and XOR operation on pixels between blocks. Hence, encryption algorithm obtained depend on Josephus problem (JP-DCCS) and double chaos cycle shift.

Ibrahim Yasser et al. [23] presented chaotic multimedia encryption technique for secure data transmission using 2D modification models. For both the confusion and diffusion rounds, a perturbation data encryption is proposed. For media encryption, a hybrid chaotification structure is utilized, in which numerous maps are included. The control parameters of the diffusion and confusion methods are generated using blended chaotic maps. Chirikov standard map model is utilized to produce the chaos sequence. This algorithm employed distinct maps, namely, the finance and galaxy maps. Before the main round, the pixel values of an image are transformed into a 1D array in a columns-wise direction. The last is split into two halves, first and second parts, every one with a length of $(\frac{M*N}{2})$, where M and N are the image dimensions. After the first circular is completed, a middle cipher image is shaped, which is next turned into a one dimension matrix for the next ciphering round via row-wise pixel value direction. When the second round is finished, the final cipher image is recovered.

3. COMPARATIVE ANALYSIS OF ALGORITHMS

Table 1 demonstrates the comparison of previous chaotic cryptosystems.

Table 1. Comparative Analysis of Algorithms Using Cameraman Image.

Ref.	Key space	Histogram distribution	Entropy	Correlation Coefficient			UAC	NPCR	SPNR	MSE
				Vertical	Horizontal	Diagonal				
[1]	$>2^{178}$	Fairly Uniform	7.9972	-	-	-	-	-	-	-
[2]	2^{300}	Fairly Uniform	7.9973	-	-	-	33.53	99.60	-	-
[3]	2^{512}	Fairly Uniform	7.9972	−0.0054	0.0047	0.0016	33.65	99.61	8.39	9488.81
[5]	$>2^{100}$	Fairly Uniform	7.9974	9.39e-04	0.0029	4.89e-05	33.45	99.62	-	-
[7]	2^{370}	Fairly Uniform	R 7.9033 G 7.9152 B 7.9980	−0.0014	0.0001	0.0005	33.78	99.99	-	-
[10]	2^{672}	Fairly Uniform	7.9998	-0.00291	0.00021	-0.00106	33.18	99.16	-	-
[11]	$>2^{100}$	Fairly Uniform	7.9971	0.00072	0.00022	0.0048	33.48	99.57	-	-
[12]	$>2^{711}$	Fairly Uniform	7.9973	5.0920e-04	6.9973e-04	0.0023	33.45	99.61	-	-
[13]	$>2^{100}$	Fairly Uniform	7.9993	−0.0046	0.0065	−0.0017	33.31	99.63	-	-
[14]	2^{26952}	Fairly Uniform	7.9975	0.0036	−0.0001	0.0073	33.49	99.64	87.04	-
[19]	$>2^{1014}$	Fairly Uniform	7.9991	$38.02*10^{-2}$	$33.61*10^{-2}$	$-27.11*10^{-2}$	33.64	99.65	8.38	9445.44

4. CONCLUSION

This document covers a variety of cryptographic techniques that make use of various chaotic maps within the period (2011-2021). Higher-dimensional maps provide more security in chaotic maps than lower-dimensional maps. When the key used in image pixel diffusion and confusion is both random and depending on the plain image, the image cryptosystem will be extremely secure. There is still a lot of work to be done in the field of multimedia cryptography. Depending on the encryption performance of various methods, each algorithm offers advantages and drawbacks. Some features of the image cryptography algorithm are included after analyzing the research documents listed above. Each of these algorithms utilize chaotic maps of various size to obtain secure image cryptosystem. Using chaos maps of varying sizes, the image can be ciphered in a variety of ways at varied speeds. The above algorithms are as well resistant to a variety of attacks, as shown by the security analysis. This paper also compares the performance of various chaos based image encryption schemes. As an inference it can be concluded that each of the cryptography algorithm is unique in its own way and the quantitative requirement is determined by the application.

ACKNOWLEDGEMENTS

The authors would like to thank Mustansiriyah University (https://uomustansiriyah.edu.iq Baghdad- Iraq) for its support in this work.

REFERENCES

1. G. Veena and M. Ramakrishna, “A Survey on Image Encryption using Chaos-based Techniques”, Int. J. Adv.Comput. Sci. Appl., vol. 12, no. 1, pp. 379–384, 2021, doi: 10.14569/IJACSA.2021.0120145.
2. Ziad M. Abood, Zainab M. Essa, "Increase Security of Image Encryption Depends on Change Pixel Location". J College of Basic Education J., Mustansiriyah University, vol. 23, No. 98, 2017.
3. A. A. Maryoosh, R. A. Mustafa, and Z. S. Dhaief, “Review: Image Encryption Techniques based on Chaotic Map”, Int. J. Eng. Res. Adv. Technol., vol. 05, no. 09, pp. 01–05, 2019, doi: 10.31695/ijerat.2019.3559.
4. X. Y. Wang, Y. Q. Zhang, and X. M. Bao, “A novel chaotic image encryption scheme using DNA sequenceoperations”, Opt. Lasers Eng., vol. 73, pp. 53–61, 2015, doi: 10.1016/j.optlaseng.2015.03.022.

5. L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion", Opt. Lasers Eng., vol. 91, no. April 2016, pp. 41–52, 2017, doi: 10.1016/j.optlaseng.2016.10.012.
6. R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps", Opt. Lasers Eng., vol. 96, no. January, pp. 39–49, 2017, doi: 10.1016/j.optlaseng.2017.04.009.
7. Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption", Signal Processing, vol.97, pp. 172–182, 2014, doi: 10.1016/j.sigpro.2013.10.034.
8. X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations", Opt. Lasers Eng., vol. 88, pp. 197–213, 2017, doi: 10.1016/j.optlaseng.2016.08.009.
9. S. F. Chiou, H. T. Pan, E. F. Cahyadi, and M.S. Hwang, "Cryptanalysis of the Mutual Authentication and Key Agreement Protocol with Smart Cards for Wireless Communications", Int. J. Netw. Secur., vol. 21, no. 1, p. 100, 2019, doi: 10.6633/IJNS.201901.
10. R. H. Al-Hashemy and S. A. Mehdi, "A new algorithm based on magic square and a novel chaotic system for image encryption", J. Intell. Syst., vol. 29, no. 1, pp. 1202–1215, 2020, doi: 10.1515/jisys-2018-0404.
11. R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata", Opt. Lasers Eng., vol. 71, pp. 33–41, 2015, doi: 10.1016/j.optlaseng.2015.03.007.
12. K. Gupta and S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", J. Inf.Secur., vol. 02, no. 04, pp. 139–150, 2011, doi: 10.4236/jis.2011.24014.
13. R. E. Boriga, A. C. Dăscălescu, and A. V. Diaconu, "A new fast image encryption scheme based on 2D chaotic maps", IAENG Int. J. Comput. Sci., vol. 41, no. 4, pp. 249–258, 2014.
14. A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm", J. Supercomput., vol. 75, no. 10, pp. 6663–6682, 2019, doi: 10.1007/s11227-019-02878-7.
15. R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map", Inf. Secur. J., vol. 25, no. 4–6, pp. 162–179, 2016, doi: 10.1080/19393555.2016.1212954.
16. K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, "Image Encryption Scheme Based on a Generalized Arnold Map and RSA Algorithm", Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/9721675.
17. M. Kaur and V. Kumar, "Beta Chaotic Map Based Image Encryption Using Genetic Algorithm", Int. J. Bifurc. Chaos, vol. 28, no. 11, 2018, doi: 10.1142/S0218127418501328.
18. U. S. Choi, S. J. Cho, and S. W. Kang, "New color image encryption for medical images based on three dimensional generalized chaotic cat map and Combined Cellular Automata", Adv. Sci. Technol. Eng. Syst., vol. 5, no. 2, pp. 104–110, 2020, doi: 10.25046/aj050213.
19. Hao. Li, L. Deng, and Z. Gu, "A Robust Image Encryption Algorithm Based on a 32-bit Chaotic System", IEEE Access, vol. 8, pp. 30127–30151, 2020, doi: 10.1109/ACCESS.2020.2972296.
20. Y. Zhang and Y. Tang, "A plaintext-related image encryption algorithm based on chaos", Multimed. Tools Appl., vol. 77, no. 6, pp. 6647–6669, 2018, doi: 10.1007/s11042-017-4577-1.
21. Heba G. Mohamed, Dalia H. El-Kamchouchi and Karim H. Moussa, "A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences", Entropy 2020, 22(2), 158; https://doi.org/10.3390/e22020158
22. Rui Wang, Guo Qiang, and Xue Feng Duan, "An image encryption scheme based on double chaotic cyclic shift and Josephus problem", Journal of Information Security and Applications, vol. 58, 2021, doi:10.1016/j.jisa.2020.102699.
23. I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications", Entropy, vol. 22, no. 11, pp. 1–23, 2020, doi: 10.3390/e22111253.

*Corresponding Author: dr.ziadmabood@uomustansiriyah.edu.iq