Eng. &Tech.Journal, Vol. 33,Part (B), No.2, 2015

Image Encryption Based on Hyperchaotic Liu system Algorithm

Dr. Alia Karim
Computer Sciences Department ,University of Technology/ Baghdad.
Email:hassanalia2000@yahoo.com
Shams Mahmoud
Computer Sciences Department ,University of Technology/ Baghdad.
Email:uot_ai_13@yahoo.com

Revised on:26/5/2014 & Accepted on: 8/1/2015

ABSTRACT:

In this paper a proposed method to encrypt images based Liu Hyper Chaotic System (LHCS) is presented. In the proposed algorithm is used to generate a key for diffusion process, to confuse relationships between the input image and encrypted image. Besides of the four initial state (initial keys) in LHCS, six control parameters were used to increase the key space. Simulation results show that the proposed method has large key space (key space is 10^{70}), and it is responsive to a trivial change of the key. Therefore it with stands different types of attacks such as brute force, differential, and chosen-cipher text attacks.

Keywords: encryption; chaotic; liu ; keyspace ; image; decryption

خوارزمية تشفير الصورة بالاعتماد على نظام ليوالاكثر فوضوية

المقدمة

في هذا البحث اقتراح خوارزمية تشفير صورة بالاعتماد على نظام ليوالاكثر فوضوية. الطريقة المقترحة تعمل على توظيف نظام ليوالاكثر فوضوية لتوليد مفاتيح السرية تسخدم لتشفير الصورة بعملية الانتشار لتفكيك العلاقة بين الصورة الاصلية والصورة المشفرة. بالاضافة الى اربعة قيم اولية (اربعة مفاتيح اولية) في نظام ليوالاكثر فوضوية استخدمت ستة المعلمات السيطرة كلها لزيادة فضاء المفتاح المستخدم لعملية التشفير . أخيرا تم اختبار خوارزمية تشفيرالصورة المقترح وفقا لتحليل الأمن وطرق معتمدة يتم استخدامها في هذا المجال. وقد اظهرت النتائج أن خوارزمية تشفيرالصورة المقترح هو آمن حسابيا. نتيجة تحليل الأمن لخوارزمية تشفير تبين أن لديه حجم المفتاح رئيسي كبير (حجم مفتاح عملية النشر هو (10^{70})) ، وأنه حساس لتغير الطفيف بالمفتاح لذلك فإنه يقاوم أنواع مختلفة من الهجمات مثل هجوم القوة, الهجوم التفاضلي, الهجوم الإحصائي وهجمات الصورة المشفرة المختارة .

INTRODUCTION

For rapid evolution of multimedia technology, and network services (ecommerce, electronic advertising, video and other types). Despite the importance of multimedia technology, but it has caused a number of problems for its users as a problem of information security and infringement of the right of ownership. To minimize these problems, a number of research proposals and secure

https://doi.org/10.30684/etj.33.2B.5
2412-0758/University of Technology-Iraq, Baghdad, Iraq

algorithms have been submitted [1]. Recently, there are many encryption schemes for the digital image information. Chaos based image encryption is the one which more interesting to researcher because the cryptographic properties in chaotic system such as control parameters, sensitivity to initial conditions, and unknown behavior [2]. Selective Encryption (SE) is a technique in multimedia encryption used to reduce computation process [3]. In this paper, proposed image encryption algorithm with diffusion operation using key generate based on LHCS. LHCS has a high level of disorder than existing chaotic systems due to the high value of its two positive Lyapunov Exponents [4] .

Liu Hyperchaotic System(LHCS)

The LHCS is one of the important models of four dimensional hyperchaotic systems which described mathematically is by system equation-1 , [4, 5]:

$$\left.\begin{aligned}
\frac{dx}{dt} &= a\,(Y-X)\\
\frac{dy}{dt} &= b\,X - e\,XZ + W\\
\frac{dz}{dt} &= -cZ + f\,X^2\\
\frac{dw}{dt} &= -d\,X
\end{aligned}\right\} \tag{1}$$

where

X, Y, Z, and W are the state variables and *a*, b, c, d, e, *f* are positive constants which represent control parameter. The system equation(1) is hyperchaotic when *(a* =10,*b* =40,*c* = 2.5, *d* =10.6,e =1 and *f* = 4). The hyperchaotic behavior of the system equation(1) is described in Figure (1).

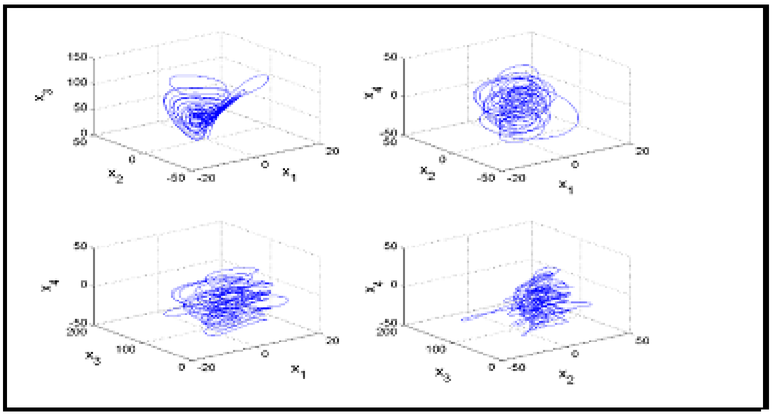


Figure (1):LHCS behavior

Discrete Cosine Transform(DCT)

domain. It uses the existing DCT on the block, because this algorithm reduces the amount of data required for re-digital image. The optical properties of the image at low frequencies, while the details are placed in the higher frequencies. The human visual system (HVS) is less than the most sensitive to higher frequencies. In the upper left corner of the matrix DCT contains a value that is always of a very large size and low frequency coefficient is called direct current (DC). All others represent an increase in the vertical and horizontal frequencies higher, called Alternating Current (AC) coefficient and become less size as they move from left to right or from top to bottom. This means that during the performance of DCT on the image in the spatial domain, the representation of focus in the upper left corner of the matrix DCT, with the lower right transactions contain less important information [6].

Assuming an 8x8 (image block) the forward (2-D) discrete cosine transforms equation (2) [3]:

$$G_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^{7} \sum_{y=0}^{7} p_{xy} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right) \qquad (2)$$

$$Where \quad C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0, \\ 1, & f > 0 \end{cases}$$

where

C_f is C_i, C_j and P_{xy} are the values of image component i,j= 0,1,...,7, x,y = 0,1,…,7. the Inverse DCT (IDCT), using equation (4), where Ci, C_j as indicated by equation-3 [6]

$$p_{xy} = \frac{1}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} C_i C_j G_{ij} \cos\left(\frac{(2x+1)i\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) \qquad (3)$$

Quantization

Quantization is the process of minimize the number of bits required to store an integer value by reducing the precision of an integer. Each position in the matrix element DCT, which is the corresponding value in the quantization matrix gives the quantum value. Actual formula is represented by equation(4)and(5) [7]:

$$Quantized\ value\ (i,j) = round\ [Dct\ coefficients\ / Q\ matrix] \qquad (4)$$

$$q(i,j) = INT[f(x,y) / qm(i,j)] \qquad (5)$$

Where

INT : rounding to the nearest integer, $qm(i,j)$: coefficient of inter and intra matrices, $q(i,j)$ final output of quantization process, and $f(x,y)$ DCT coefficients.

The inverse quantization can found by equation -6.where $q^{-1}(i,j)$ represents the inverse quantization.

$$q^{-1}(i,j) = f(x,y) = INT\ [qm(i,j) * q(i,j)] \qquad (6)$$

The Proposed Image Encryption Method

The proposed image encryption method consiste of two main steps, including: Key Generation Based on LHCS, selective image encryption. The details of each step are described in the following subsections.

Key Generation Based On LHCS

To explain the key generation based on LHCS solving via fourth order Runge-Kutta(Rk-4) in detail, several steps will be illustrated .

a. Numerical Method For LHCS

The 4th order Runge-Kutta (RK-4) is used for resolving the continuous LHCS because it produces a more accurate estimate of the solution.The numerical solution is described by the following steps:

Step 1: Initialization

This is covered by system equation (1), where n number of iteration time, where n is a constant.

h= time step=0.0005, **X_0=X, Y0=Y, Z0=Z, W0=W** as initial values, initial state of the Liu chaotic system, **a, b, c, d, e** as initial control parameters.

Step 2: In this step, Pre-iterate LHCS is for n. In order to compute the solutions of the Liu hyperchaotic system the following sub steps is used:

Step 2.1:

Compute the initial slopes kj, mj, lj, and pj, where j=1, and the step h is chosen as 0.0005, defined by system equations (7):

$$\left.\begin{aligned} k_j &= a\,(Y_n - X_n) \\ m_j &= b\,X_n - e\,X_n Z_n + W_n \\ l_j &= -cZ + f\,X^2{}_n \\ p_j &= -d\,X_n \end{aligned}\right\} \quad (7)$$

At the next clock cycle, the system passes to the next step 2.2.

Step2.2:

Compute the initial slopes kj, mj, lj, and pj, where j=2, 3, and the step h is chosen as 0.0005, defined by system equations (8):

$$\left.\begin{aligned} k_j &= a[\,(Y_n + hk_{j-1}/2) - (X_n + hk_{j-1}/2)\,] \\ m_j &= b(X_n + hk_{j-1}/2) - e[(Z_n + hk_{j-1}/2) \times (X_n + hk_{j-1}/2)] + (w_n + hk_{j-1}/2) \\ l_j &= c(Z_n + hk_{j-1}/2) + f(x_n + hk_{j-1}/2)^2 \\ p_j &= d(x_n + hk_{j-1}/2) \end{aligned}\right\} \quad (8)$$

Step2.3:

Compute the initial slopes kj, mj, lj, and pj, where j=4, and the step h is chosen as 0.0005 defined by system equations (9):

$$\left.\begin{array}{l} k_j = a[\,(Y_n + hk_{j-1}) - (X_n + hk_{j-1})\,] \\ m_j = b(X_n + hk_{j-1}) - e\,[(Z_n + hk_{j-1}) \times (X_n + hk_{j-1})] + (w_n + hk_{j-1}) \\ l_j = -c(Z_n + hk_{j-1}) + f(x_n + hk_{j-1})^2 \\ p_j = -d(x_n + hk_{j-1}) \end{array}\right\} \quad (9)$$

Step2.4

In the final sub step, compute the next hyper chaotic solution values, defined by system equations (10):

$$\left.\begin{array}{l} X_{n+1} = X_n + \frac{h}{6}(k_0 + 2k_2 + 2k_3 + k_4) \\ Y_{n+1} = Y_n + \frac{h}{6}(l_0 + 2l_2 + 2l_3 + l_4) \\ Z_{n+1} = Z_n + \frac{h}{6}(m_0 + 2m_2 + 2m_3 + m_4) \\ W_{n+1} = W_n + \frac{h}{6}(p_0 + 2p_2 + 2p_3 + p_4) \end{array}\right\} \quad (10)$$

All steps are repeated so that chaotic digital are obtained at the output**.**

b. Key Generation

In this stage**,** the LHCS is iterated continuously to obtains four keys stream elements from the current state according to the following system equations (11):

$$\left.\begin{array}{l} KX_n = mod\,((abs\,(x_n) - floor\,(abs\,(x_n))) \times 10^{14},\, 256) \\ KY_n = mod\,((abs\,(y_n) - floor\,(abs\,(y_n))) \times 10^{14},\, 256) \\ KZ_n = mod\,((abs\,(z_n) - floor\,(abs\,(z_n))) \times 10^{14},\, 256) \\ KW_n = mod\,((abs\,(w_n) - floor\,(abs\,(w_n))) \times 10^{14},\, 256 \end{array}\right\} \quad (11)$$

Where

N number of iterations, abs(x_n) returns the absolute value of X. Floor(x) finds the nearest integer less than or equal to X, mod(x, y) get remainder after division [8,9]**.** All the variables are declared as 64-bit double-precision type, which has a 15-digit precision according to the IEEE floating-point standard, and therefore the decimal fractions of the variable is multiplied by 10^{14}(11) , and The function assumed that the 256 gray scale image for this reason mod on 256.The output from this stage four keys for each iteration time to decrypted first (DC, 3AC) for each block. The output from this stage is four keys for each iteration time (n) used in partial encryption as the next sub section in the diffusion process.

Selective Image Encryption

A proposed selective encryption approach(shown in figure2) is applied to first 2×2 sub block (first DC and the first three AC coefficients) for each block using the key generated via LHCS Diffusion process steps are:

1. Prepare image (Loading and Reading a bitmap image, then Transforming RGB format into YCrCb color space format).
2. Decomposing Y component (luminance component) into 8×8 blocks.

3. Transforming each block from spatial to frequency domain by adopting DCT .
4. Quantizing DCT coefficients to the nearest integer value.
5. Diffusion key generation based on LHCS.
6. Encryption the first (2×2) sub block for each block (DC and the first three AC coefficients (diffuse coefficients using Xor operation)
7. Applying DCT inverse.
8. Reconstructing encrypted Y' component form 8×8 blocks, Finally, Transforming Y'CrCb color space format into an encrypted RGB image format. Figure systems.

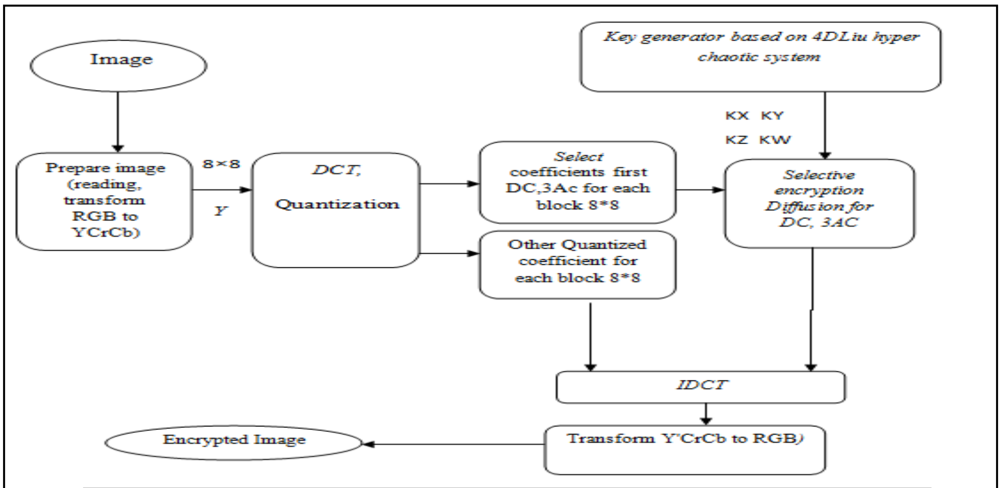
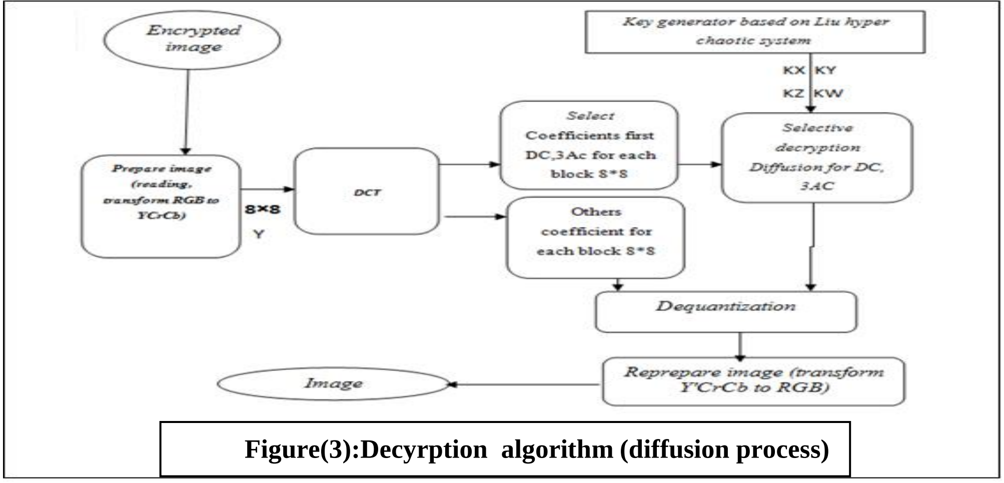


Image
Key generator based on 4DLiu hyper chaotic system
KX KY
KZ KW
Prepare image (reading, transform RGB to YCrCb)
8×8
Y
DCT, Quantization
Select coefficients first DC,3Ac for each block 8*8
Selective encryption Diffusion for DC, 3AC
Other Quantized coefficient for each block 8*8
IDCT
Transform Y'CrCb to RGB)
Encrypted Image

Figure(2):Proposed Encryption algorithm (diffusion prosess)

The decryption algorithm is similar to the encryption algorithm. Figure 3 show decryption algorithm (diffusion process) based on LHCS.

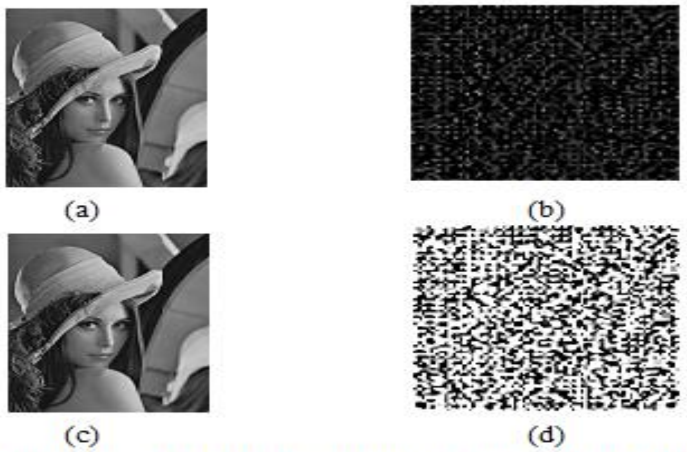

Encrypted image
Key generator based on Liu hyper chaotic system
KX KY
KZ KW
Prepare image (reading, transform RGB to YCrCb)
8×8
Y
DCT
Select Coefficients first DC,3Ac for each block 8*8
Selective decryption Diffusion for DC, 3AC
Others coefficient for each block 8*8
Dequantization
Reprepare image (transform Y'CrCb to RGB)
Image

Figure(3):Decyrption algorithm (diffusion process)

Experimental Results

The proposed algorithm was implemented and the experimental analysis of the proposed algorithm presented in this paper has been done with several images. Figure

4 shows the experimental results with "lena.bmp" image. Figure 4 (a) original image. Figure 4(b) is its encrypted image with the encryption initial key *(x_0, y0, z0, w0)=(30,30,30,30),and control parameter(a,b,c,d,e,and f)=(10,40,-2.5,-10,1,4) with* as can be see, the encrypted image is rough and unknowable. Figure 4(c) is the decrypted image by use of the decryption algorithm with the same key (correct key). It can be seen that the decrypted image is clear and correct without any distortion. But if we use the wrong key, we will get an unexpected image. For example, Figure4(d) shows the decrypted image using the wrong initial key *(x_0, y0, z0, w0)*=(30.00000000001,*30,30,30) ,and control parameter(a,b,c,d,e,and f)=(10,40,-2.5,-10,1,4).* So it can be concluded that LHCS is responsive to the key, a little change of the key will generate a completely different decryption result and cannot get the correct original image.



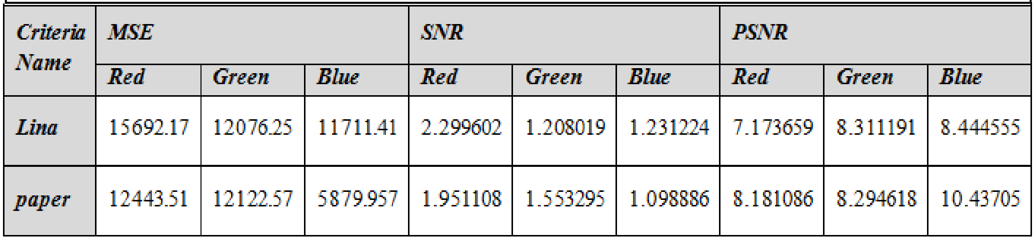
Figure(4):Image encryption and decryption experimental result:(a)origin image,(b)encrypted image,(c)decrypted image by correct key,(d)decrypted image by wrong Key.

The encryption algorithm proposed in the paper has the ability to resist brute-force attack since the key space for the proposed algorithm is ($10^{14×5}$=10^{70}), where 5 for the hyperchaotic initial value *(x_0, y_0, z_0, w_0, N)* as the original key, and each digit has 14 digital numbers, therefore, it can be seen that the new chaotic image encryption algorithm is good at resisting brute-force attack.

to prove that the proposed algorithm has the ability to hide the pure image information and in the same time when reconstruct the original image from deciphered one without loss any information a set of test measurements are used and the result shown in table (1).

Measurements which used for test are MSE (Mean Square Error), SNR (Signal to Noise Ratio) and PSNR (Peak Signal to Noise Ratio). Large values of MSE stand for the key is able to hide pure image information while the small values of SNR and PSNR stand for the key caused large error result in high image suppression of original image information [12].

(1)Table (1): The Test Results of diffusion Key encryption to make Dffusion process



Criteria Name	*MSE*			*SNR*			*PSNR*		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*	*Red*	*Green*	*Blue*
Lina	15692.17	12076.25	11711.41	2.299602	1.208019	1.231224	7.173659	8.311191	8.444555
paper	12443.51	12122.57	5879.957	1.951108	1.553295	1.098886	8.181086	8.294618	10.43705

From table (1) it can conclude the following points:

1- Large values of MSE mean that proposed key is able to hide pure image information (there are large changes in ciphered image caused by the use of *diffusion key* based on LHCS generator).

2. Small values of SNR and PSNR mean the proposed key caused large noise (i.e. small values cause high image suppression of original image information.

Conclusions

To overcome the drawbacks of small key space and weak security in the widely used image encryption, this paper propose an image encryption algorithm based on LHCS with SE technique. Experimental analysis demonstrates that the proposed algorithm shows advantages of large key space and high-level security (MSE, SNR and PSNR). The algorithm presented in this paper can be widely applied in any information security fields.

References

[1]. A Hyper-chaos Based Image Encryption Algorithm. zaiping, Chen, et al. Tianjin, China : s.n., 2010.

[2]. A NEW DIGITAL IMAGE ENCRYPTION ALGORITHM. Huang, Xiaoling. Zhanjiang, 524088, Guangdong, P.R. CHINA : s.n., 2012, Vol. 80, pp. 609-616. 4.

[3]. Two-Level Image Encryption Algorithm Based on Qi. Bazeb, Sandra and Qi, Guoyuan. Pretoria, South Africa : s.n., 2012.

[4]. ADAPTIVE CHAOS CONTROL AND. Vaidyanathan, Sundarapandian. Avadi, Chennai-600 062, Tamil Nadu, INDIA : s.n., June 2011, Vol. 1. 2.

[5]. HYBRID CHAOS SYNCHRONIZATION OF. Vaidyanathan, Sundarapandian. Avadi, Chennai-600 062, Tamil Nadu, INDIA : s.n., June 2011, Vol. 1. 2.

[6]. A Selective Image Encryption Based on Chaos Algorithm. Matti Yousif, Dr. Abeer and Mohammed Ali, Manaf. Journal of KerbalaUniversity:s.n., 2013, Vol. 11. 1.

[7]. Design and Implementation of Secure Public Key. Karim Abdul Hassan, Dr. Alia and Salim Mouhamad, Ghadah. Eng. & Tech. Journal : s.n., 2010, Vol. 28. 3.

[8]. Design and FPGA implementation of a wireless. Sadoudi, Said, et al. 2013, Vol. 43.

[9]. A new image encryption algorithm based on hyper-chaos. Gao, Tiegang and Chen, Zengqiang. Department of Automation, Nankai University, Tianjin 300070, PR China : s.n., 2008, pp. 394–400.

[10]. New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos. Li-hong, LEI, Feng-ming, BAI and Xue-hui, HAN. Changchun,China : s.n., 2013.

[11]. A Symmetric Chaos-Based Image Cipher with an Improved. Fu, Chong, et al. China; : s.n., 2014, pp. 770-788.

[12]. Partial Cryptography in Digital Media Environment Based on. B. Abdul Wahab, Hala and Ali Sameer, Rafal. Baghdad, Iraq : s.n., 2013, Vol. 54, pp. 455-467. 2.