Chaotic Modeling and Simulation (CMSIM) 4: 571-581, 2013

Chaos Cryptography: Relation Of Entropy With Message Length and Period

George Makris[1], Ioannis Antoniou[2]

Complex Systems Analysis Laboratory, Mathematics Department, Aristotle University, 54124, Thessaloniki, Greece
[1]E-mail: georgmak@outlook.com
[2]E-mail: iantonio@math.auth.gr

Abstract: Chaos cryptography is implemented by torus automorphisms with strictly positive entropy production. For any given entropy production $h > 0$ we explicitly construct integer valued automorphisms with entropy $\mathsf{h}(S) \geq \mathsf{h}$. We identify compatibility conditions between the values of the entropy production and the lengths of the messages in terms of the grid size and we propose constructive ways to encrypt messages of arbitrary length in terms of torus automorphisms with any given desired entropy production. We moreover prove that the restrictions of chaotic maps with the same entropy have the same period for a fixed grid size.
Keywords: Entropy, Cryptography, Chaos, Cryptography with Chaos.

1. Introduction

Chaos cryptography was proposed by Shannon in his classic 1949 mathematical paper on Cryptography where used chaotic maps as models - mechanisms for symmetric key encryption. Of course Shannon did not employ the term Chaos which emerged in the 1970s. This remarkable intuition was based on the paradigm of the Baker's map introduced by Hopf in 1934 as a simple deterministic mixing model with statistical regularity. Shannon observed that using chaotic maps, encryption is achieved via successive mixing of the initial information which is uniformly "spread" all over the available state space. In this way it is becoming exponentially hard to recover the initial message if the reverse transformation is not known. Baker's map is the simplest example of chaotic Torus Automorphisms with constant Entropy production equal to one bit at every step. The Entropy production theory of Torus Automorphisms and general Chaotic maps was developed later by Kolmogorov and his group [Arnold and Avez, 1968; Katok ea, 1995; Lasota ea, 1994], following Shannon's earlier foundation of Information Theory in 1948. Baker's map has also served as a toy model for understanding the problem of Irreversibility in Statistical Mechanics [Prigogine, 1980]. Chaos cryptography with 2-dimensional maps deal with image encryption [Guan D. ea, 2005; Xiao G. ea , 2009] and text encryption [Kocarev ea, 2003; Kocarev ea, 2004; Kocarev L. and Lian S., 2011;Li S., 2003]. We have proposed a new implementation method for

Received: 30 April 2013 / Accepted: 10 October 2013

ISSN 2241-0503

Chaos Cryptography based on Chaotic torus automorphisms, applicable for both image and text encryption simultaneously [Makris G, Antoniou I, 2012a] and designed torus automorphisms with desired entropy production [Makris G, Antoniou I, 2012b]. Part of these results is summatized in section 1.
As the grid discretizations of chaotic Torus automorphisms are periodic, for effective implementation we have to examine the conditions for reliable cryptography implementation. The objectives of this work are: a) to examine the dependence of the period on the entropy production and on the grid size (Section 2), b) to provide conditions for admissible grid discretizations (Section 3) and c) to provide algorithms for the construction of integer torus automorphims with desired entropy production (Appendix A) and for adapting the image size to the appropriate grid size (Appendix B) for customized implementation of chaotic cryptography).

The automorphisms of the 2-torus $Y=[0,1)\times[0,1)$ are defined by the formula:

$$S: Y \to Y: \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\, 1), n \in \mathrm{N} \quad \textbf{(1)}$$

Where $\mathrm{A}=\begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{bmatrix}$ is a real invertible matrix with inverse: $\mathrm{A}^{-1}=\dfrac{1}{\mathrm{ad}-\mathrm{bc}}\begin{bmatrix} \mathrm{d} & -\mathrm{b} \\ -\mathrm{c} & \mathrm{a} \end{bmatrix}$

Chaotic Torus automorphisms (1) have one eigenvalue greater than 1, according Pesin's 1977 Formula.

Lemma:

1) The class of chaotic automorphisms (1) with $\mathrm{ad}-\mathrm{bc}=1$ consists of the matrices:

$$A=\begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \dfrac{ad-1}{b} & \mathrm{d} \end{bmatrix}, a \in \mathrm{R}, b \in \mathrm{R}-\{0\}, d > 2-a \quad \textbf{(2)}$$

2) The entropy production of the Chaotic automorphisms (2) is:

$$\mathsf{h}=\log_2 \lambda_1 = \log_2 \frac{(\mathrm{a}+\mathrm{d})+\sqrt{(\mathrm{a}+\mathrm{d})^2-4}}{2} = \log_2 \frac{tr(A)+\sqrt{(tr(A))^2-4}}{2},$$
$$a \in \mathrm{R}, b \in \mathrm{R}, d > 2-a \ (\text{or } tr(A) > 2) \quad \textbf{(3)}$$

3) The chaotic automorphisms (2) are expressed in terms of the entropy production as a parameter h by the formula:

$$A=\begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \dfrac{\mathrm{a}\cdot\left(2^{\mathsf{h}}+2^{-\mathsf{h}}-\mathrm{a}\right)-1}{b} & 2^{\mathsf{h}}+2^{-\mathsf{h}}-\mathrm{a} \end{bmatrix}, \mathrm{a} \in \mathrm{R}, b \in \mathrm{R}-\{0\},\ \mathsf{h}>0 \quad \textbf{(4)}$$

4) For the class of chaotic automorphisms A with one eigenvalue greater than 1 and $\mathrm{ad}-\mathrm{bc}=-1$ we have the corresponding formulas:

$$A=\begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \dfrac{ad+1}{b} & \mathrm{d} \end{bmatrix}, a\in \mathrm{R}, b\in \mathrm{R}-\{0\}, d>-a \quad \textbf{(5)}$$

$$\mathrm{h}=\log_2 \lambda_1=\log_2 \frac{(\mathrm{a}+\mathrm{d})+\sqrt{(\mathrm{a}+\mathrm{d})^2+4}}{2}=\log_2 \frac{tr(A)+\sqrt{(tr(A))^2+4}}{2},$$
$$a\in \mathrm{R}, b\in \mathrm{R}, d>-a \ \ (\text{or } tr(A)>0) \quad \textbf{(6)}$$

$$A=\begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \dfrac{\mathrm{a}\cdot\left(2^{\mathrm{h}}-2^{-\mathrm{h}}-\mathrm{a}\right)+1}{b} & 2^{\mathrm{h}}-2^{-\mathrm{h}}-\mathrm{a} \end{bmatrix}, \mathrm{a}\in \mathrm{R}, b\in \mathrm{R}-\{0\}, \ \mathrm{h}>0 \quad \textbf{(7)}$$

Formulas (2),(3),(4) are proven in [Makris G, Antoniou I, 2012b]. The corresponding formulas for the case $\mathrm{ad}-\mathrm{bc}=-1$ are obtained in a similar way. From formulas (3),(6) we see that

Corollary

Two Chaotic Torus Automorphisms have the same Entropy Production (are isomorphic), if and only if they have the same trace

2. Entropy production and the period of the discretization restrictions of integer Torus Automorphisms

The implementation of cryptographic algorithms requires discretization of the chaotic maps onto the selected $N\times N$ grid. In order to preserve the grid structure we shall consider torus automorphisms with integer matrix elements. Given a desired entropy production value not less than h we may construct integer torus automorphisms with entropy production h from formulas (4),(7) using the algorithms presented in appendix A.

The coordinates of pixels are elements of the NxN lattices $\acute{\mathrm{A}}_N\times\acute{\mathrm{A}}_N$. The restriction of any integer torus automorphism to $\acute{\mathrm{A}}_N\times\acute{\mathrm{A}}_N$ (mod N):

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=A\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\, N)=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\, N) \quad \textbf{(8)}$$

is a periodic transformation, called the NxN discretization automorphism of (1). The period of the discretization automorphisms (8) is the minimal number T which satisfies the formula:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^T(\mathrm{mod}\, N)=\mathrm{I}_2=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (9)$$

Theorem 1: All discretization automorphisms (8) with the same trace have the same period T which depends only on the size N of the grid.

Proof:
First we shall show that the discretization automorphisms (8) of isospectral matrices have the same period. It is enough to show that the matrices A (9) and

$$\Delta = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \textbf{(10)}$$

define discretization automorphisms (8) with the same period.
We have:

$$A = B^{-1} \cdot \Delta \cdot B$$

Where B is a diagonalization transformation of A.
If T is the period of (8), from (9) and (10) we have:

$$A^T = \left(B^{-1} \cdot \Delta \cdot B\right)^T = B^{-1} \cdot \Delta^T \cdot B$$

and:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^T (\mathrm{mod}\, N) = \left(B^{-1} \begin{bmatrix} {\lambda_1}^T & 0 \\ 0 & {\lambda_2}^T \end{bmatrix} B \right) (\mathrm{mod}\, N) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore:

$$\begin{bmatrix} {\lambda_1}^T & 0 \\ 0 & {\lambda_2}^T \end{bmatrix} (\mathrm{mod}\, N) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore the discretizations (8) of Δ and A have the same period T. From the eigenvalue formulas (3) and (6), we see that the eigenvalues λ_1, λ_2 depend only on the trace of A. Therefore any two matrices with the same trace define discretizations (8) with the same period. ■

3. Entropy Production and Grid size

We observe that torus automorphisms with different entropy production may have identical discretizations (8). For example, applying formula (6) we see that the torus automorphisms with matrices $A_1 = \begin{bmatrix} 2 & 1 \\ 4093 & 2047 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 2 & 1 \\ 93 & 47 \end{bmatrix}$ have entropy productions $h_1 = 11.0007$ and $h_2 = 5.6141$ correspondingly. However their discretizations (8) to the grid 100×100 are identical:

$$\begin{bmatrix} 2 & 1 \\ 4093 & 2047 \end{bmatrix} \mathrm{mod}\, 100 \equiv \begin{bmatrix} 2 & 1 \\ 93 & 47 \end{bmatrix} \mathrm{mod}\, 100 .$$

The same is true for the grids 200×200, 500×500, 1000×1000 and others.
This is an undesirable fact because only equivalent chaotic torus automorphisms should have identical grid discretization (8). We found that this requirement is true only for certain values of the entropy production h and grid size N. The result is the following:

Theorem 2: An necessary and sufficient condition for one to one correspondence between torus automorphisms and their grid discretizations (8) is: $N > \max\{a,b,c,d\}$ **(11)**

Equivalently in terms of entropy production, using (3) and (6) we have the conditions:

$$N > \max\left\{a, b, 2^h + 2^{-h} - a, \frac{a\cdot\left(2^h + 2^{-h} - a\right) - 1}{b}\right\} \text{ for } \det(A) = 1 \quad \textbf{(12)}$$

$$N > \max\left\{a, b, 2^h - 2^{-h} - a, \frac{a\cdot\left(2^h - 2^{-h} - a\right) + 1}{b}\right\} \text{ for } \det(A) = -1 \quad \textbf{(13)}$$

Prof:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\, N) = \begin{bmatrix} a\ (\mathrm{mod}\, N) & b\ (\mathrm{mod}\, N) \\ c\ (\mathrm{mod}\, N) & d\ (\mathrm{mod}\, N) \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\, N) =$$

$$= \begin{bmatrix} \upsilon_\alpha & \upsilon_b \\ \upsilon_c & \upsilon_d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\, N)$$

As the remainders $\upsilon_\alpha, \upsilon_b, \upsilon_c, \upsilon_d$ are always not greater than a,b,c,d correspondingly, we have: $tr\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a + d \geq \upsilon_\alpha + \upsilon_d = tr\begin{bmatrix} \upsilon_\alpha & \upsilon_b \\ \upsilon_c & \upsilon_d \end{bmatrix}$

Therefore, from (3) and (6) we have: $h\begin{bmatrix} a & b \\ c & d \end{bmatrix} \geq h\begin{bmatrix} \upsilon_\alpha & \upsilon_b \\ \upsilon_c & \upsilon_d \end{bmatrix}$

$h\begin{bmatrix} a & b \\ c & d \end{bmatrix} = h\begin{bmatrix} \upsilon_\alpha & \upsilon_b \\ \upsilon_c & \upsilon_d \end{bmatrix}$ if and only if: $a < N$ and $b < N$ and $c < N$ and $d < N$, from which follows the desired result. ■

The natural question now arises what are the possible values of entropy production for automorphisms satisfying (11)

Without significant loss of generality we consider the simpler class of integer torus automorphisms with $b = 1$. Formulas (12) and (13) are written :

$$\boxed{h < \log_2\left[\left(a+N\right) + \sqrt{\left(a+N\right)^2 - 4}\right] - 1 \ ,\ 0 < a < N}\ ,\ \det(A) = 1 \quad (14)$$

$$\boxed{h < \log_2\left[\left(a+N\right) + \sqrt{\left(a+N\right)^2 + 4}\right] - 1\ ,\ 0 < a < N}\ ,\ \det(A) = -1 \quad (15)$$

Therefore given the grid size N we know the maximal entropy production from (14),(15) for automorphisms with b=1 and conversely given a desired entropy

production value we know the minimal grid size from (12),(13). The relation between entropy production and grid size is shown in figure 1. We shall call the discretizations (8) with grid size $N \times N$ admissible discretizations if and only if the conditions (12) , (13) hold.

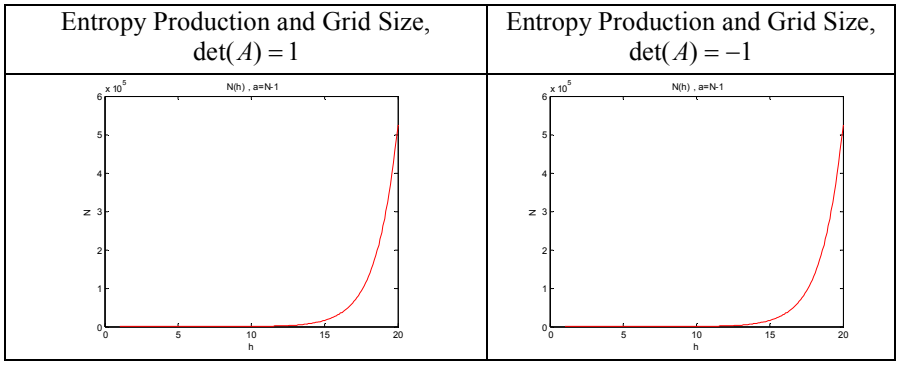

Figure 1: Entropy Production and Grid Size

In case the grid $N \times N$ for admissible discretization (8) of the constructed torus automorphisms is larger than the message size $n \times m$ we may enlarge and adapt the message size to the grid size using the algorithm presented in appendix B.

5. Conclusions

After extending our previous results [Makris G, Antoniou I, 2012b] on the entropy production on torus automorphisms (Lemma and Corollary), we show that the period of grid discretizations of chaotic automorphisms depends only on the entropy production and on the grid size (Theorem 1). In order to avoid the undesirable fact that torus automorphisms with different entropy production may have the same discretization, we provide a necessary and sufficient condition of admissible grid discretizations (Theorem 2). For customized implementation of chaotic cryptography, we provide algorithms for the construction of integer torus automorphims with desired entropy production (Appendix A) and for adapting the image size to the appropriate grid size (Appendix B). These results are necessary for implementation of chaotic cryptographic algorithms of desired entropy production. Based on Theorem 2 and Appendix B we can automatically adapt the message size to admissible discretization for effective cryptography.

References

1. Akritas P., Antoniou I., Pronko G., "On the Torus Automorphisms: Analytic Solution, Computability and Quantization", Chaos, Solitons and Fractals 12,(2001) 2805-2814

2. Arnold, V. I. and Avez, A., Ergodic Problems of Classical Mechanics Benjamin, New York , 1968

3. Guan Z. H., Huang F., and Guan W.. Chaos-based image encryption algorithm. Physics Letters A, Vol. 346, Issues 1-3,(2005), pp 153-157.
4. Dyson FJ, Falk H., Period of a discrete cat mapping. Am Math Monthly 1992;2(99):603-14
5. Hopf E., On Causality, Statistics and Probability, J. Math. and Phys. 13, (1934), 51-102.
6. Katok A., Hasselblatt B., Introduction to the Modern Theory of Dynamical Systems, Cambridge University Press, Cambridge, UK , 1995
7. Kocarev L., Sterjev M., Amato P., RSA ENCRYPTION ALGORITHM BASED ON TORUS AUTOMORPHISMS, IEEE, ISCAS (2004), IV 577-580.
8. Kocarev L., Tasev Z., and Makraduli J., "Public-Key Encryption and Digital-Signature Schemes Using Chaotic Maps", 16th European Conference on Circuits Theory and Design, September 1 – September 4, 2003, Krakow, Poland, ECCTD 2003.
9. Kocarev, L., Lian, S., Chaos-Based Cryptography. Theory, Algorithms and Applications,Studies in Computational Intelligence, Vol. 354, (2011), ISBN 978-3-642-20542-2, Berlin.
10. Lasota A. and Mackey M., Chaos, Fractals, and Noise, Springer-Verlag New York, 1994.
11. Li, S., Analyses and New Designs of Digital Chaotic Ciphers. Ph.D. thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, 2003
12. Makris G., Antoniou I., 2012, "Cryptography with Chaos", Chaotic Modeling and Simulation (CMSIM), VOL 1: 169-178, 2012, ISSN 2241-0503.
13. Makris G., Antoniou I., 2012, "Cryptography with Entropy Producing Maps", 6th World Congress of NonLinear Analysts, IFNA 2012, 25 June - 1 July, Athens, Greece
14. Pesin Ya. B., Characteristic Lyapunov exponents and smooth ergodic theory, Russ. Math. Surv. 32:4, (1977), 55-112
15. Prigogine I., From Being to Becoming, Freeman, New York, 1980
16. Shannon C. , A Mathematical Theory of Communication. Bell System Technical Journal, vol. 27, pp. 379–423, 623–656 (1948); Shannon C. and Weaver W., Mathematical Theory of Communication, Univ of Illinois Press, Urbana, Ill (1949).
17. Shannon, C., Communication Theory of Secrecy Systems. Bell System Technical Journal, Vol.28, Issue 4, (1949), pp 656–715.
18. Smale S., "Differentiable dynamical systems". Bulletin of the American Mathematical Society 73: (1967) 747–817.
19. Smale S., Finding a horseshoe on the beaches of Rio, Mathematical Intelligencer 20, (1998), 39-44
20. Xiao, D., Liao, X., Wei, P., Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons & Fractals, Vol. 40, Issue 5, (2009), pp 2191-2199.

Appendix A: Construction of integer torus automorphisms with entropy production not less than any desired positive real number

Torus automorphisms have been applied to NxN grids and the periods has been related to the grid size N [Vivaldi, 1989; Dyson FJ and Falk H, 1992; Akritas ea, 2001;Antoniou ea, 1997; Xiao ea, 2009]. According to formula (2) we should have $\frac{ad-1}{b} \in Z$ for any integer values a,b,d. , ie. : $(ad) mod\, b = 1$

For any given entropy production $h > 0$ we construct integer matrixes A with entropy $h(A) \geq h$ according to the following algorithm.

Algorithm 1. Construction of integer matrices A with $\det(A) = 1$

Step 0: inputs: $h \in (0, \infty)$, a,$b \in$ Z

Step 1: Set $x = \lceil tr(A) \rceil = \lceil 2^h + 2^{-h} \rceil$, $\lceil z \rceil$ is the ceiling of z

Step 2: Set d=x-a

Step 3: if [d>2-a and (b=1 or $(ad)\ mod\ b = 1$)] goto Step 9

Step 4: if [$a\ mod\ b \neq 0$ and $b\ mod\ a \neq 0$] goto Step 7

Step 5: Set x=x+1 and d=x-a

Step 6: goto Step 3

Step 7: Set a=a+1 and d=x-a

Step 8: goto Step 3

Step 9: return $A = \begin{bmatrix} a & b \\ \frac{ad-1}{b} & d \end{bmatrix}$

Step 10: return $\lambda_1(A) = \frac{(a+d) + \sqrt{(a+d)^2 - 4}}{2}$

Step 11: return $h(A) = \log_2 \lambda_1(A)$

Input			Output		
h	a	b	$A=\begin{bmatrix} a & b \\ \frac{ad-1}{b} & d \end{bmatrix}$	$\lambda_1(A)$	$h(A)$
1.2	1	1	$A=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$	2.6180	**1.3885**
1.2	2	3	$A=\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$	3.7321	**1.9000**
3.5	1	1	$A=\begin{bmatrix} 1 & 1 \\ 10 & 11 \end{bmatrix}$	11.9161	**3.5748**
3.5	5	1	$A=\begin{bmatrix} 5 & 1 \\ 34 & 7 \end{bmatrix}$	11.9161	**3.5748**
3.5	5	3	$A=\begin{bmatrix} 5 & 3 \\ 13 & 8 \end{bmatrix}$	11.9161	**3.5748**
11	2	1	$A=\begin{bmatrix} 2 & 1 \\ 4093 & 2047 \end{bmatrix}$	2049	**11.0007**

Table 1: Examples of **Algorithm 1**

According to formula (4) we should have $\frac{ad+1}{b}\in Z$ for any integer values a,b,d. , ie. : $(ad+1) mod\, b=0 \Rightarrow (ad) mod\, b=b-1$

Algorithm 2. Construction of integer matrices A with $\det(A)=-1$

Step 0: inputs: $h\in(0,\infty)$, a,$b\in$ Z

Step 1: Set $x=\lceil tr(A)\rceil=\lceil 2^h-2^{-h}\rceil$, $\lceil z\rceil$ is the ceiling of z

Step 2: Set d=x-a

Step 3: if [d>-a and (b=1 or $(ad)\ mod\ b=b-1$)] goto Step 9

Step 4: if [a $mod\ b\neq 0$ and $b\ mod\ a\neq 0$] goto Step 7

Step 5: Set x=x+1 and d=x-a

Step 6: goto Step 3

Step 7: Set a=a+1 and d=x-a

Step 8: goto Step 3

Step 9: return $A=\begin{bmatrix} a & b \\ \frac{ad+1}{b} & d \end{bmatrix}$

Step 10: return $\lambda_1(A)=\frac{(a+d)+\sqrt{(a+d)^2+4}}{2}$

Step 11: return $h(A)=\log_2\lambda_1(A)$

Input			Output		
h	a	b	$A=\begin{bmatrix} a & b \\ \frac{ad+1}{b} & d \end{bmatrix}$	$\lambda_1(A)$	$h(A)$
1.2	1	1	$A=\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$	2.4142	**1.2716**
1.2	2	3	$A=\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$	3.3028	**1.7237**
3.5	1	1	$A=\begin{bmatrix} 1 & 1 \\ 12 & 11 \end{bmatrix}$	12.0828	**3.5949**
3.5	5	1	$A=\begin{bmatrix} 5 & 1 \\ 36 & 7 \end{bmatrix}$	12.0828	**3.5949**
3.5	5	3	$A=\begin{bmatrix} 5 & 3 \\ 12 & 7 \end{bmatrix}$	12.0828	**3.5949**
11	2	1	$A=\begin{bmatrix} 2 & 1 \\ 4093 & 2046 \end{bmatrix}$	2048	**11.0000**

Table 2: Examples of **Algorithm 2**

Appendix B: Algorithm to Enlarge image size from $(n\times m)$ to $(N\times N)$:

Step 0: inputs: $(image, N, c)$, N: new image size, c: color of new pixels

Step 1: calculate (n,m) =image size

Step 2: $W_h = N-n$

Step 3: Create an new blank image1 with size $\left(\frac{W_h}{2}\times m\right)$ and color c to every pixel.

Step 4: Create an new image2 with vertical quote of three images: $image2=\begin{pmatrix} image1 \\ image \\ image1 \end{pmatrix}$. Image2 size=$(N\times m)$

Step 5: $W_w = N-m$

Step 6: Create a new blank image3 with size $\left(\frac{W_w}{2}\times N\right)$ and color c to every pixel.

Step 7: Create a new_image with horizontal quote of three images : $new\_image = (image3 \quad image2 \quad image3)$. new_mage size= $(N \times N)$

Image (342 x 454)	**Image1** (79 x 454)	**Image2** (500 x 454)	**Image3** (500 x 23)
			
Inputs	**New_image** (500 x 500)		**Output**
Image N=500 c=white Calculations $W_h = N - n = 158$ $W_w = N - m = 46$			New_image

The advantage of adding pixels in an image is to keep the original information.