A Novel Gray Image Encryption Algorithm Based on Modified Transcendental Equation

Li Tu
School of Information Science and Engeering,Hunan City University,Yiyang,Hunan 413000,China
Email:tulip1903@163.com

Yan Wang, Ni Li,Saiqiu Guo
School of Information Science and Engeering,Hunan City University,Yiyang,Hunan 413000,China
Email: shaoguanzai@sina.com,lini66600079@163.com,saiqiu8105@tom.com

***Abstract*—In this paper a modified transcendental equation is proposed, and we analyzed its chaotic characteristics and periodic. It is a simple non-linear mode, l but it has complex dynam ics.Then it was used in gray image encryption. This is a digital image encryption algorithm, dual scrambling that based on chaos of pixel position and pixel value.Compared with the traditional transcendental equation, the improved transcendental equation has only chaos characteristic, when the number of iterations is less than 5, the equation has periodicity,and when iterative times are more than 20, the equation has chaotic characteristic only, so the modified transcendental equation has larger key space.Performance test and security analysis are performed using key space analysis, the pixels distribution character, correlation coefficients, the ability to resist attack and key sensitivity test. Results suggest that the proposed image encryption scheme is secure and efficient, with high potential to be adopted for the secure image communication applications.**

***Index Terms*—transcendental equation,key space, strange attractors, period-doubling bifurcation**

I. Introduction

In recent years, owing to frequent flow of digital images across the world over the transmission media, people can obtain, use or process digital images more frequently. It has become essential to secure them from leakages. Since digital media such as image, audio, and video are easy to process, copy and transfer, the emergence of powerful tools raises a series of problems. To protect the information within the digital images from the attacks of intruders is becoming a more and more serious problem. The requirements to fulfill the security needs of digital images have led to the development of good encryption techniques.

Encryption is an ideal solution of this problem. It is also called image scrambling, which produces an unintelligible or disorder image from the original image. But because of the certain characteristics of digital images, such as redundancy of data, strong correlation among adjacent pixel, less sensitive comparing to the text data, especially the large quantities of data and the requirement of real-time processing, traditional ciphers such as DES, AES, RSA etc. it is not suitable for the encryption of this kind of data. To solve this problem, new encryption algorithms derived from chaotic systems are proposed and owning to the important properties of chaotic systems, such as the sensitive dependence on initial conditions and pseudo- random array which is hard to predict after a certain times of iteration.

The existing image encryption algorithms can be classified into two kinds. One is spatial-based method; the other is frequency-based method. The spatial-based algorithms are usually achieved by swapping the pixel positions or altering pixel values. Since optical encryption based on double-random-phase encoding was firstly proposed by Refregier and Javidi [1], many techniques, such as digital holography [2], Fresnel transform [3], and fractional Fourier transform [4], have been used for encryption. The widely used method is double-random-phase encoding in Fourier domain or fractional Fourier domain [1]. And the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques.

"Chaotic encryption" is first brought forward by A.Robert and J.Matthews[5]. After that, some new chaotic encryption algorithms were proposed[6-9]. In this paper, the authors attempt to use a modified transcendental equation to make the confusion and diffusion and use 8 type of operations to encrypt the original image.

II. Chaos and improved transcendental equation

2.1 The Concept of Chaos

Chaos is a particularly interesting non-linear effect. It is a kind of non-periodic motion, and it almost relates to each branch of natural science and social science.

In 1963 Lorenz [10] found the first canonical chaotic attractor and it has been intensively studied. It has been detected in a large number of dynamic systems of various physical natures. It has been said that something as small as the flutter of a butterfly ’s wing can ultimately cause a typhoon halfway around the world, which means that

© 2013 ACADEMY PUBLISHER
doi:10.4304/jsw.8.9.2336-2343

beyond two or three days, the world’s weather forecasts are speculative, and beyond six or seven days they are worthless.

In 1975 Li Tien-Yien and J.A.York have proposed an idea of "Period 3 Implies Chaos" [11], if a system has 3 period, then the system should have any positive integer cycles. In 1978 J Feigenbaum has found two universal constants from period-doubling bifurcation to chaos[12], in 1981 F. Takens, a Holland mathematician have introduced the renormalization group theory,and put the method of determining strange attractors[13]. In 1987 Grassber P has put the method of reconstituting dynamical systems, and analysed a chaotic system by extracting fractional dimension , Lyapunov exponents and other characteristic values from time series[14], in 2005,Wang Xingyuan has built two-dimensional Logistic mapping with one-order terms and two-order terms, and he has revealed the universality of the transformation from regular motion state to chaos of nonlinear complex systems by using phase space reconstruction and quantitative criterion of chaos[15].

In 1997 Fridrich has put forward a chaotic image encryption idea for the first time. Then chaos theoretical analysis got into practical application[16-22], a number of chaos based image encryption scheme have been developed in recent years which we discuss in brief in this paragraph[23-29].

In our life, we describe the static, simple, reversible natural using Newtonian mechanics, while the real world is dynamic, random, irreversible. Therefore, chaos is a foundational discipline of researching on the process, rather than researching on the states, and it is a discipline of researching on the evolution, rather than researching on existence. The following are the characteristics of chaotic systems

(1). Scenarios: In 1981,Eckmann identified three main scenarios: the first one is the scenarios of period-doubling bifurcation, and it is called Feigenbaum scenarios; The second is an intermittent chaos model, and it is called Pomeau-Manneville scenarios; the third is the Hopf bifurcation scenarios,and it is called Ruelle-Takens-Newhouse scenarios.

(2). Phase space: In continuous dynamic systems, we describe the system using a group of first-order differential equations, the phase space of the system is customized the axis with state variables. A state of the system is represented with a point in the phase space, there is only one integral curve through this points.

(3). Chaotic motion: It is a kind of highly unstable motion. It is a deterministic system and it is limited in a finite phase space. The strong instability of the track means that the similar track will separate as time increases. Because of this instability, the long-term behavior of the system will show some kind of chaotic characteristics.

(4). Fractal and fractal dimension: The fractal is a kind of geometric properties of point-set in n-dimensional space.

These point-sets have unlimited fine structure. In any scale, it has self-similarity and global similarity, and they have non-integer dimensions that are smaller than the number of dimensions. Fractal dimension is to describe the basic properties of fractal quantitatively using non-integer dimension and fractal.

(5). Fixed point: It is called balance point, steady state. Fixed point is a set of values taken from system state variables, for these variables , the system does not change with time. In continuous dynamic systems, there is a point x_0 in a phase space,if when $t \to \infty$,and $x(t) \to x_0$,then x_0 is a fixed point

(6). Attractor: It is a point-set s (or a subspace). In this point-set, for almost any point in neighborhood S, when $t \to \infty$,all track line tends to neighborhood S.Attractor is a stable fixed point

(7). Strange attractor: It is called chaotic attractor, a collection of the fractal attractors in the phase space. A series of points make up this collection and it is not periodically. These chaotic orbit run in these attractor set.

(8). Bifurcation and bifurcation point: It is called branch which means when one or a group of parameters change, the type of long time dynamics motion also changes. This parameter (or this group of parameters) is a bifurcation point. In the bifurcation point, small changes in parameters will bring different dynamic characteristics, so in the bifurcation point, the system is unstable.

(9).Periodic solution: For a system $x_{n+1} = f(x_n)$, when $n \to \infty$,if $\xi = x_{n+i} = x_n$, then this system has periodic solution ξ . A fixed point can be regarded as a solution of period 1 because it satisfies the equation $x_{n+1} = x_n$.

(10). The initial value sensitivity: Sensitive dependence on initial conditions is a basic feature of chaotic system, and someone use it to define the chaos: A chaotic system is the e system whose ultimate state sensitively depends on its initial state. An important consequence of the initial value sensitivity is to make the long-time behavior of the system become unpredictable.

The characteristics of the chaotic mappings have attracted the attention of cryptographers to develop new encryption algorithms. As these chaotic maps have many fundamental properties such as ergodicity, mixing property and sensitivity to initial condition/system parameter and which can be considered analogous to some cryptographic properties of ideal ciphers such as confusion, diffusion, balance and avalanche property etc.

2.2 Transcendental Equation and Logistic Mapping

In 1976,an American Mathematical ecologists May R put forward the famous insect population model, which was called "Logistic mapping". The one-dimensional Logistic mapping is one of the most simple forms of a chaotic mapping[2]. The mathematical expression of Logistic mapping is:

$$x_{k+1} = ux_k(1-x_k), k = 0,1,2,... \quad (1)$$

here $x_k \in (0,1), \mu \in (0,4]$,parameter μ is a bifurcation parameter. Figure 1(a) is the scatter plot of a Logistic mapping.

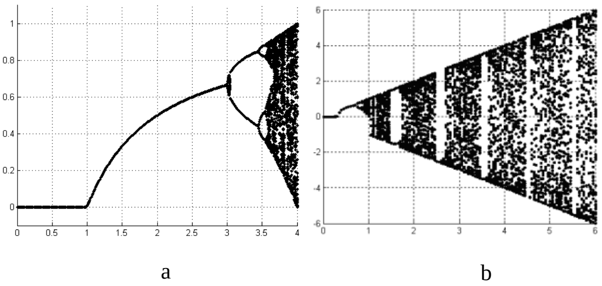

Figure 1.Bifurcation and Blank window for Logistic mapping (a) and transcendental equation (b)

When parameter $\mu=1+\sqrt{8}=3.828...$,there are 3 periodic solutions in Logistic mapping, According to the theory of "Period 3 Implies Chaos" that have been proposed by Li Tien-Yien and J.A.York,in the interval of $[\mu,4]$, There are periodic windows.

The Logistic mapping, like any one-dimensional map, is a rule for getting a number from a number.When parameter $\mu<1$, no matter what initial values we choose, the final result will be close to 0.When parameter $1<\mu<3$, the final result will be close to $1-\frac{1}{\mu}$,in the range of $1<\mu<3$,x=0 and $x=1-\frac{1}{\mu}$ are two fixed points. And when $\mu<1$,x=0 is the stable point, when μ=1, the Logistic mapping becomes unstable and forks, μ=1 is the bifurcation value. when μ>1, x=0 becomes the unstable point , and $x=1-\frac{1}{\mu}$ is the stable point. When $\mu=3$, the Logistic mapping becomes unstable and forks once more, in the range of $3<\mu<1+\sqrt{6}$ the iterative value x falls between two fixed values, a solution of period 2 (One time of iterative calculation is a cycle), this corresponds to the limit cycle in Continuous dynamics system, so when μ =3,period doubling bifurcation(Hope bifurcation) appears in the Logistic mapping. In the range of $1+\sqrt{6}<\mu<3.544090359$,the system is in steady state again when $\mu=3.54409035\,9$, the second time period doubling bifurcation(Hope bifurcation) appears in the Logistic mapping, there is a solution of period 4 in the process of iterative calculation when the value of parameter μ continue to increase, there will be solutions of period 8, period 16 and period 32 etc. t's period-doubling bifurcation in the process of iterative calculation .

When the value of parameter μ reaches the maximum $\mu=3.56994567\,2$, the bifurcation cycle of the system is 2^{∞}, the system reaches a chaotic state, when $\mu>4$,it is an unbounded function. The parameter μ is fixed, but if one studies the map for different values of μ (up to 4, else the unit interval is no longer invariant) it is found that μ is the catalyst for chaos.

In the process of iterative calculation above, parameter μ_1 indicates the bifurcation value from period 1 to period 2 ,that is $\mu_1=3$, and parameter μ_2 indicates the bifurcation value from period 2 to period 4 ,that is $\mu_2=1+\sqrt{6}\approx 3.449898743$, By calculating the ratio of spacing $(\mu_n-\mu_{n-1})/(\mu_{n+1}-\mu_n)$,n=2,3,4…,we can get the result in table 1.

TABLE 1.

SPACING RATIO OF PERIOD-DOUBLING BIFURCATION

The bifurcation of Logistic mapping	Bifurcation values μ_n	Spacing ratio $\frac{(\mu_n-\mu_{n-1})}{(\mu_{n+1}-\mu_n)}$
1→2	3	
2→4	3.449487743	4.751466
4→8	3.544090359	4.656251
8→16	3.564407266	4.668242
16→32	3.568759420	4.66874
32→64	3.569691601	4.6691
64→128	3.569891259	4.66
128→256	3.569934019	4.66
…	…	…
periodic solution →chaos	3.569945672	4.669201661

Function 2 is a transcendental equation, Feigenbaum has studied its bifurcation and chaotic characteristics, and made its corresponding figure.

$$x_{k+1}=\lambda\sin(\pi x_k),k=0,1,2,... \quad (2)$$

In function 1,parameter λ is a non-negative real number, from any initial value $x_0\in[0,1]$, after iterative computation, we can obtain a certain sequence x1, x2, ... Xn. When the parameters in the range [0,6],so the x coordinate is [0,6]; the value of y have negatives, so the y coordinate is [-6,6],the bifurcation and blank window for transcendental equation is shown in Figure 1(b).

For different values of parameter λ, the equation(1) will present different characteristics, with the increase of the parameter λ, the system experiences period-doubling bifurcation continuously, and reaches the chaos eventually, the specific process is as follows:

When parameter λ is in the range of [0,0.3],the value of y keeps at 0, then it begins to increase; when parameter λ is in the vicinity of 0.75, the function curve gets into two branches. With the increasing of parameter λ, the iterative sequences is more complex, the iterative results may fall in any sub-interval of the interval (-6,6) randomly, and it may be repeated. This is the ergodicity of chaos. With the increasing of parameter λ, the function curve shows a periodicity.

2.3Improved Transcendental Equation

We proposed an improved transcendental equation, its mathematical expression is:

$$x_{k+1}=\lambda\sin(\pi u x_k(1-x_k)),k=0,1,2,... \quad (3)$$

In fact, we have introduced a Logistic chaotic mapping, and had it as a parameter of the transcendental equation. In order to ensure that the parameter of the sine function is a chaotic sequence, we selected the following range of parameters $\mu \in [3.7,3.99]$ and $\lambda \in (0,3)$, then we made the following function diagram, the bifurcation and blank window for the improved transcendental equation is shown in Figure 2.

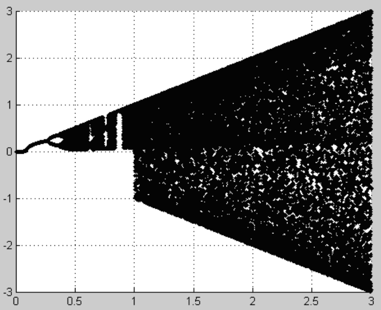

Figure 2.Bifurcation and Blank window for the improved transcendental equation

In order to analyze the modified transcendental equation further, we have studied its number of iterations and chaos range. Took an initial value x0=0.123456,when the number of iterations was taken a minimum of 1 or 2,the modified transcendental equation is a simple linear function, when the number of iterations is from 3 to 5, its scatter plot are like 3 sine waves, the waveform diagram is as Figure 3(c).

It can be seen from Figure 3(c),when the number of iterations is low, the function has significant cycle characteristics, but not chaotic characteristics. when the number of iterations is 20, and we took the results of 15-20 times iterative, the waveform diagram is as Figure 3(d). It can be seen from the Figure 3(d), the function has only chaotic characteristics ,but no cycle characteristics.

We amplified the range of parameter λ, when the range of parameter λ is (0,100),the number of iterations is 200, and we took the results of 120-150 times iterative, the waveform diagram is as Figure 3(e), the function has chaotic characteristics only.

When the parameters λ is in the range of (90,100), after iterative computation, we can get the scatter plots as Figure 3(f), Figure 3(f) is the enlarged Figure 3.e.

Figure 3 shows that when the number of iterative is more than 20, the function has significant chaotic characteristics, and no cycle characteristics. This is because in the modified transcendental equation, the parameter is a Logistic mapping, it is a chaotic sequence, and the chaotic sequence destroys the periodicity of sine function. In order to ensure the chaotic characteristics of the function, we control the parameters μ in the range of (3.8,3.999),and we take the value the after 100 times of iterations, so the function has no periodicity.

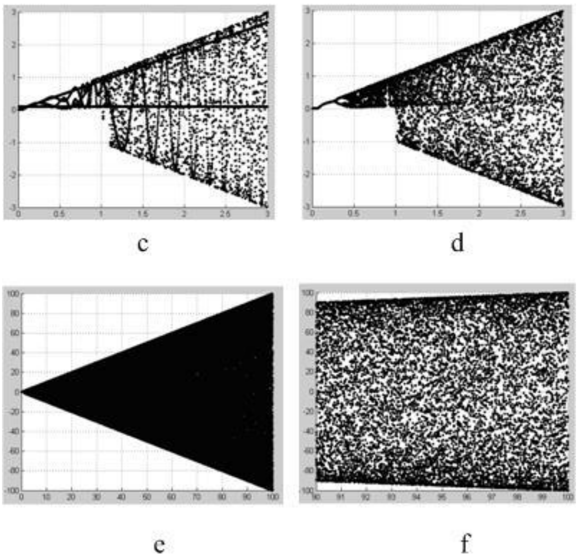

Figure 3. Bifurcation for the improved transcendental equation after 1-5 times(c) and 20 times(d) of iterative computation,Bifurcation for the transcendental equation after 100 times iterative computation and parameter λ in the range of 0-100(e) and parameter in the range of 90-100(f)

III. Performance analysis

3.1 Distribution Characteristics

The values are not evenly distributed in the range of chaotic sequence. Different chaos function have different distribution characteristics, and the same chaotic equation have the same distribution characteristics. We studied the modified transcendental equation and the traditional logistic equation, when we took the initial value x0=0.12345678, λ=10 and parameter μ=3.900001,and calculated 65535(256*256) iterative results, the distribution of their values is shown in Table 1.The experimental results show that the distribution of the modified transcendental equation is more concentrated than that of the traditional logistic mapping and the traditional transcendental equation. Its iterative results are more random, so the modified transcendental equation has better distribution characteristics.

This transcendental equation is modified by a sine function, so there will be negative numbers in its range, and it has periodic. Figure 3 shows that , when parameter λ>1, a negative chaotic sequence will be obtained. Because the chaotic sequence that iteratived through Logistic mapping is in the range of (0,1), so the changing of parameter λ makes the negative value, and because Logistic mapping is a chaotic mapping, it was used as a parameter in a transcendental equation, and it destroyed the periodicity of the sine function.

The key space of modified transcendental equation is [1.5,+∞], the key of the traditional Logistic mapping is (3.56 ... , 4],and the key of the transcendental equation is (1 , +∞]. Compared with a transcendental equation, the modified transcendental equation has no periodicity, and compared with a Logistic mapping, the range of the modified transcendental equation is very large. So the key space of modified transcendental equation is very large.It is easy to realize the function in hardware. Figure 3(e) shows the bifurcation for the transcendental equation after 100 times iterative computation and parameter λ in the range of 0-100 ,and Figure 3(f) shows the bifurcation f and parameter in the range of (90-100).

TABLE 2

DISTRIBUTION CHARACTERISTICS

	Improved transcendental equation		Transcendental equation		Logistic mapping	
Initial value	x0=0.12345678 u=3.900001 λ =10		x0=0.12345678 u=3.900001 λ =10		x0=0.12345678 u=3.900001	
Interval	Number	Percentage	Number	Percentage	Number	Percentage
(-2,2)	8823	13.46%	11631	17.75%	65535	100%
(-4,-2)&(2,4)	8951	13.65%	9044	13.80%	0	0
(-6,-4)&(4,6)	9721	14.83%	9408	14.35%	0	0
(-8,-6)&(6,8)	11595	17.69%	10940	16.69%	0	0
(-10,-8)&(8,10)	26446	40.35%	24513	37.40%	0	0

IV. ENCRYPTION ALGORITHM AND DECRYPTION SCHEME

In this algorithm a chaotic sequence was generated using the modified transcendental equation, and we changed position and pixel value of the pixel of an original image, this enhances the security. The system is sensitive to the initial value x_0, the initial value x_0, parameter λ, parameter μ, and the iteration number can be used as a key. If the attacker does not know the exact key, or there are subtle differences between the attack key and the real key. There will be a great difference in the key sequence, bringing a great deal of difficulty to the attacker. In fact, the sensitivity of the system to the initial value x_0 ,parameter λ and parameter μ, can achieve 10^{-14}.

4.1. Encryption Algorithm

Step 1）Read a size of 256*256 pixels grayscale image M, converted M to a length of 256*256 one-dimensional sequence A1.

Step 2）Selected the initial value x_0 =0.400001, μ=3.900001, λ=93, we discarded the results before 1000 times iterative operation which generated chaotic sequence L1 from a modified transcendental equation, this is a length of 256*256 one-dimensional sequence too. We changed all numbers in sequence L1 into absolute values, and then divided sequence A1 by parameter λ, and sequence L1 has been converted into a chaotic sequence in range of [0,1].

Corresponded the various elements in sequence A1 and sequence L1, built a two-dimensional matrix p, its column length is 2, and its line length is 65536(256* 256). We put the elements of sequence L1 on the first row of the matrix P, elements of A1 on the second line, the two-dimensional matrix p is also the decryption matrix. Then sorted the elements in the L1, that sort the first line of matrix P, took the second line of sorted matrix P1, we got a one-dimensional sequence A3. The position of elements in sequence A1 has changed following the elements in chaotic sequence L1, it has generated the ciphertext sequence A3. The decryption method is very easy, we sort the second row of ciphertext matrix P1 respectively, the first line of matrix P2 is the decryption.

Step 3）Selected the parameter μ=3.8563201,the initial value x0=0.654321 and λ=99, we discarded the results before2000 times iterative operation, it generated a length of 256*256 one-dimensional sequence L3 using the modified transcendental equation. In order to increase the difficulty of the ciphertext, took the first, the sixth and the fifth digit of the elements in sequence L3 after the decimal point to form a three-digit number, had it on 256 remainder operation, and we got sequence L5.

Step 4）XORed A3 and L5, got sequence A4, this was the grayscale encrypted ciphertext.

4.2. Decryption Scheme

The decryption needs to be divided into the following 2 steps;XORed A4 and L5, got sequence N3.this is the decryption process on gray value; Then we decrypted the cipher text using the decryption method of Step2, after reordering A5 generated N2; then we got the decrypted image.

V.EXPERIMENTAL RESULTS

Figure 4 is an original gray image and its histogram.

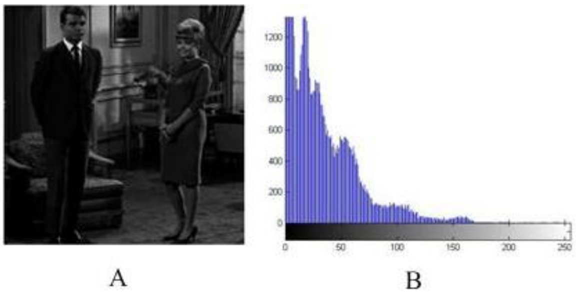

Figure 4. Original image (A) and Histogram of it (B)

Selected the initial value x0=0.400001,u=3.900001, λ=93,it generated a sequence L1 using modified transcendental equation,then scrambled the position of the original image,and encrypted it using sequence L1.Figure 5 is the image after position transformation (C) and the histogram of image after position transformation

(D).

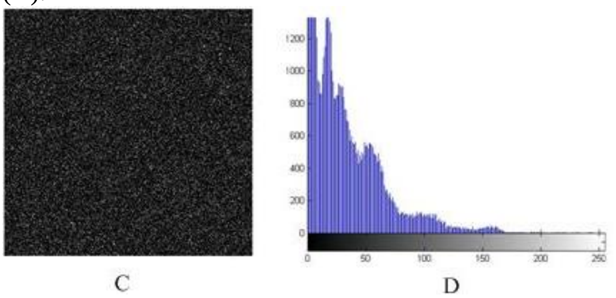

Figure 5. Image after position transformation (c) and its histogram (d)

Selected the parameter μ=3.8563201,the initial value x0=0.654321 and λ=99, through iterative calculation we got a length of 256*256 one-dimensional sequence L3 using the modified transcendental equation again.Then changed the gray value of Figure 5(C),and encrypted it using sequence L3.Figure 6 is the image after gray value encryption (E) and its histogram (F).

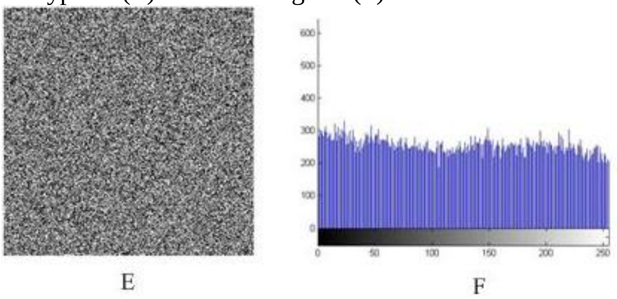

Figure 6. Image of the gray value encryption (E) and its histogram (F)

Figure 7 is the image after gray value decryption(G), the decrypted image(H) and its histogram(I).

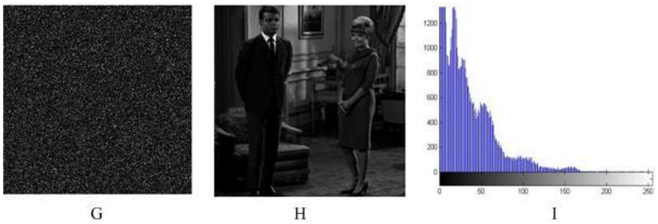

Figure 7. Image after gray value decryption, decrypted image, histogram of decrypted image

VI. Security analysis

6.1 Key Space Analysis

For a secure image encryption scheme, the key space should be large enough to make the brute-force attack infeasible. The key of this algorithm is $K = (\lambda, x_0, \mu_0)$, parameter x_0 can be taken any value in the range of (0,1), parameter μ_0 can be taken any value in the range of (3.569945672,4), and the value scope of the parameter λ is more bigger,it can reach the range of (1,∞), so the key space of the improved transcendental equation is infinite, the uncertainty of parameter λ, x_0, μ_0 increases the key space greatly.So exhaustive attacking on key K is not feasible.

In this encryption algorithm we used two-dimensional array to store digital images, The size of the image is m×n. The main operations of this encryption algorithm is to sort the sequence and to replace the pixel position and the pixel value.The time complexity of sequence sorting algorithm is $O(n^2)$,these operation of replacement is to take or assign values to two-dimensional digital image array according to the corresponding relations of a sorted sequence, so its time complexity of sequence sorting algorithm is $O(n^2)$ too,so the total time complexity of the encryption algorithm is $O(n^2)$.

6.2 Histogram Analysis

To analyze the image histogram is one way to attack the image encryption. Figure 4(B), Figure 5(D), Figure 6(F) and Figure 7(I) are the histogram of the image before and after encryption. The histogram shows, before encryption the rise and fall of the histogram is very large, the distribution is not uniform, and after encryption the histogram is complanate, the gray value of encrypted image is in uniform distribution. This shows that in the range of (0,255), the probability of the pixel value in encrypted image is equal. The statistical characteristics of encrypted image are quite different from that of the original image. The statistical characteristics of original image spread to encrypted image evenly, this reduces their correlation greatly.

6.3 Key Sensitivity Analysis

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, we discuss the security analysis of the proposed image encryption scheme such as statistical analysis, sensitivity analysis with respect to the key and plaintext, key space analysis etc. to prove that the proposed cryptosystem is secure against the most common attacks.

The key sensitivity is the degree of changing in the ciphertext when a little changing in the initial key. A good encryption algorithm should not only be sensitive to the key, but also to the plaintext, and the cipher key should uniformly distributes over the value space of ciphertext.

We studied the sensitivity of the key using renderings of matrix transformations,which can be seen from Figure 8, different values of x0 and parameter a have great impact on pixel, when slightly transform values of x0 and parameter a, we will get a quite different encrypted image. An attacker will have a great difficulty on cracking the ciphertext.

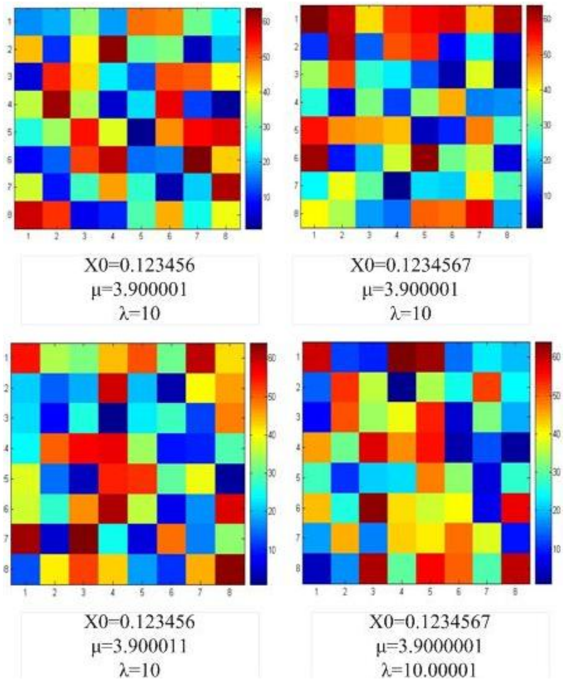

Figure 8. Diagrams of key sensitivity of modified transcendental equation

6.4 Correlation of Adjacent Pixels

The substantive characteristics of a digital image determine that there is strong correlation among adjacent pixels.This correlation makes the content of the image is easy to be identified.

We calculated the pixel correlation using the following formula(4) and formula(5):

$$\operatorname{cov}(x,y)=E((x-E(x))(y-E(y))) \qquad (4)$$

$$R_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \qquad (5)$$

Here x and y are the gray values of two adjacent pixels in the image, E(x) is a mathematical expectation, D(x) is the variance of x, cov(x,y) is the population covariance. In order to destroy the statistical attacking,we must reduce the correlation of adjacent pixels.The lower the correlation coefficient, the better the encryption effect.In the process of calculation,we use formula (6-8).

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \qquad (6)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \qquad (7)$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))\cdot(y(i)-E(y)) \qquad (8)$$

We selected 2000 adjacent pixels in the original image and the encrypted image,the distribution is shown in Figure 9 and Figure 10.The correlation among the original image pixels shows a linear distribution,the correlation among the encrypted image pixels is a random distribution.

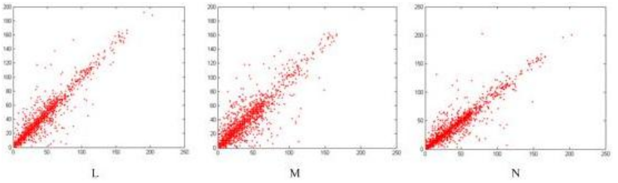

Figure 9. Correlation of level adjacent pixels (L),correlation of Horizontal adjacent pixels(M),correlation of diagonal adjacent pixels (N) for original image

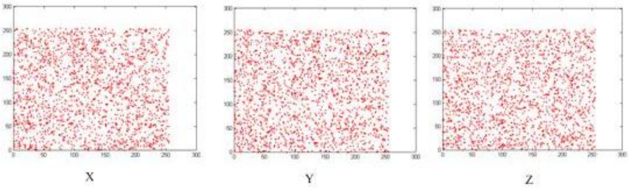

Figure 10. Correlation of level adjacent pixels(X),correlation of horizontal adjacent pixels(Y), correlation of diagonal adjacent pixels(Z) for encrypted image after the position transforming and the gray value changing

It can be seen from Figure 10 and Figure 11,the degree of image scrambling is very significant.

VII CONCLUSIONS

This paper analyzes transcendental equation chaotic image encryption algorithm, and proposes an improved encryption and decryption model based on the algorithm. The theoretical analyses show that the generated chaotic sequences has excellent performance such as cross correlation and sensitivity.It is shown by Matlab simulations,the results of experiment simulation show that the algorithm has more efficiency and security,and it has a good pseudo randomness, a low calculation complexity, a giant key space, and it is highly suitable for the multimedia data encryption.

ACKNOWLEDGMENT

This work was supported by Scientific Research Fund of Hunan Provincial Science Department under Grant (No: 2013FJ3087, 2013FJ3086), Scientific Research Fund of Hunan Provincial Education Department under Grant (No:12C0573)

REFERENCES

[1] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier planer and omencoding. *Opt Lett*, vol.20,pp.767-769, 1995.

[2] Javidi B, Nomura T. Securing information by use of digital holography. *Opt Lett*,vol.25:pp.28-30,2000.

[3] Chen L, Zhao D. Optical color image encryption by wave length multi-plexing and lensless Fresnel transform holograms. *Opt Express*,vol.14,pp. 8552-8560,2006.

[4] Liu Z, Li Q, Dai J, Sun A, Liu S, Ahmad M. A new kind of double encryption by using acutting spectrum in the 1-D fractional Fourier transform domains. *Opt Commun*, vol.282,pp.1536–1540,2009.

[5] Rober A, Matthews J, On the derivation of a "chaotic" encryption algorithm, *Cryptologia*, Vol. 13, no. 1, pp. 29-42, 1989.

[6] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process", *IJACT,* Vol. 3, no. 5, pp. 223-233, 2011.

[7] Zhiliang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences,* vol.181,no.6, pp. 1171–1186,2011.

[8] Liu Yan, Fu Chong, Fast Pseudo Stochastic Sequence Generator Based on Chebyshev Map, *Conttol Engineering of China,* vol.13,no.4,pp.377-380,2006(In Chinese).

[9] Brahim Nini, Chafia Melloul, "Pixel Permutation of a Color Image Based on a Projection from a Rotated View", *JDCTA,* Vol. 5, No. 4, pp. 302-312, 2011.

[10] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955.

[11] Lorenz E.N, "Deterministic nonperiodic flow". *Atmospheric Science,* vol.20 , pp. 130-141. 1963.

[12] Tien-Yien Li, James A. Yorke, "Period Three Implies Chaos", *The American Mathematical Monthly,* vol. 82, no. 10, pp. 985-992, 1975

[13] Feigenbaum.M.J, "Quantitative Universality for a Chaos of Nonlinear Transformations", *Journal of Statistical Physics,* vol.19, no.1,pp.25-52, 1978.

[14] Takens. F, "Detecting strange attractors in turbulence", *Lecture Notes in Mathematics,* vol.898,pp.366-381,1981.

[15] Peter Grassberger, Itamar Procaccia, "Characterization of Strange Attractors",*Phys. Rev. Lett* ,vol.50, pp. 346-349, 1983.

[16] Wang Xingyuan, Zhu Weiyong "Researches on Chaos and Fractal of the Coupled Logistic Map",*Journal of Image and Graphics,* Vol. 4(A) , No. 4, pp. 340-344, 1999 (in Chinese)

[17] Dongming Chen,Yongming Liu,Xiaodong Chen,Yunpeng Chang,Jing Wang, "A Novel Chaotic Map and DES based File Encryption Algorithm", *IJACT:International Journal of Advancements in Computing Technology,* vol.3, no.7, pp.198-205, 2011.

[18] Hu Dahui,Du Zhiguo,"An Audio Watermarking Based on Logistic Map and m-Sequence",*JDCTA: International Journal of Digital Content Technology and its Applications,*vol.6,no.8,pp.169-176,2012

[19] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps",*Chaos,SolitonsFractals,*vol.21,no.3,pp.749-761, 2004.

[20] Philippe.Refregier, Bahram.javidi, "Optical image encryption based on input plane and Fourier plane random encoding" , *Optics.Letters,* vol.20, no.7, pp.767-769,1995.

[21] B.M.Hennelly and J.T.Sheridan, "Image encryption techniques based on fractional Fourier transform" , *Proc. SPIE 5202,* pp.76-87, 2003.

[22] G.Unnikrishnan,J.Joseph,and K.Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain", *Optics Letter,* vol.25,no.12, pp.887-889, 2000.

[23] Peng Xiang, Zhang Peng, Wei Hengzheng et al, "Known-plaintext attack on optical encryption based on double random phase keys", *Optics Letter,* vol.31, no.8, pp.1044-1046, 2006.

[24] N.Bourbakis,C.Alexopoulos,"Picture data encryption using SCAN pattern", *Pattern Recogn,*vol.25, no.6, pp.567-581, 1992.

[25] Fridrich Jiri, "Symmetric ciphers based on two dimensional chaotic maps", *International journal of bifurcation and chaos,* vol.8, no.6, pp.1259-1284, 1998.

[26] N.K Pareek, Vinod Patidar,K.K Sud,"Discrete chaotic cryptography using external key",*Physics Letter A,*vol.309, no.1-2,pp.75-82,2003.

[27] Pareek N,Patidar V,Sud K,"Cryptography using multiple one-dimensional chaotic maps", *Communications in Nonlinear Science and Numerical Simulation,* vol.10, no.7,pp.715-723,2005.

[28] Pareek N,Patidar V,Sud K,"Image encryption using chaotic Logistic map", *Image and Vision Computing,* vol. 24, no.9, pp.926-934, 2006.

[29] Patidar V,Pareek N,Sud K,"A new substitution-diffusion based image cipher using chaotic standard and Logistic maps", *Communications in Nonlinear Science and Numerical Simulation,*vol.14, no.7, pp.3056-3075,2009.