African Journal of Mathematics and Computer Science Research Vol. 3(8), pp. 163- 172, August 2010
Available online at http://www.academicjournals.org/ajmcsr
ISSN 2006-9731 ©2010 Academic Journals

Full Length Research Paper

An improved chaotic encryption scheme

K. A. Ayanlowo[1], O. Folorunso[2], A. T. Akinwale[2] and A. N. Njah[3]

[1]Department of Computer Science, Moshood Abiola Polytechnic, Abeokuta, Ogun State, Nigeria.
[2]Department of Computer Science, University of Agriculture, Abeokuta, Ogun State, Nigeria.
[3]Department of Physics,University of Agriculture, Abeokuta, Ogun State, Nigeria.

Accepted 26 May, 2010

In this paper, an attempt is made to develop a functional encryption scheme by exploiting the strength and redefining the operational limits of two related existing schemes. Various parameters used for comparative assessment show that the proposed scheme is better than the existing ones in terms of functionality, strength and suitability for applications in securing messages on networks and work files on stand-alone databases.

Key words: Chaos, cryptography, logistic map.

INTRODUCTION

The failure of the existing traditional schemes such as DES and the discovery of the intrinsic relationship between chaotic systems and traditional cryptography has shifted the attention of researchers in cryptography to the use of non-linear chaotic functions (Caroll, 1991; Abir, 2008), such as skew-tent map (Alvarez et al., 1999; Kwok, 2004), logistic map (Bose, 1994; Baptista, 1998; Wong, 2002; Wong et al., 2003), henon map (Solak, 2004), lorenz map (Lawande et al., 2005) and others (Tang, 2002; Yang, 2009; Zhang, 2005) for encryption. The defining properties of chaotic systems that make them suitable for application in cryptography are ergodicity, sensitivity to slight changes in initial conditions and system parameters, noise likeness and unpredictability of the dynamics of the state variables, etc. A review of the existing literature on chaotic cryptography reveals two general approaches: Hardware and Software approaches.

The hardware approach is a synchronization-based cryptographic scheme referred to as masking and mostly applied in secure communications (Tang, 2002; Tsun-I, 2005). In secure communications, the drive and response systems serve as the transmitter and receiver respectively. The message is embedded in the chaotic dynamics of the state variables of the transmitter via a mathematical function and is recovered at the receiver via the inverse function when the drive and the response systems are synchronized (Alvarez and Li, 20004; Alvarez et al., 2004; Chee, 2004; Alvarez et al., 2005). Secure communication is assured if the dynamics of the drive system (transmitter) is complex, the encryption or masking algorithm is complex and the transmitted signal is complex (Tang, 2002). The hardware approach is, however, vulnerable to cryptographic attacks based on dynamical reconstruction of the chaotic signal using nonlinear dynamical forecasting (NLDF) methods as well as other methods (Tsun-I, 2005; Alligood, 1996; Changsong, 2000; Alvarez et al., 2004; Chee, 2004; Alvarez et al., 200).

In contrast to the foregoing, a software approach becomes more practical and in tune with present day advances in information processing. Apart from the fact that it presents some strength against attacks using reconstruction dynamical method, its implementation is also inexpensive. The scheme presented in this research work is a product of a comprehensive appraisal of some of the existing schemes (Bose, 1994; Baptista, 1998; Wong, 2002; Wong et al., 2003; Lawande et al., 2005; Masuda, 2005; Huang, 2005) vis-à-vis their strength and weaknesses. Particular attention was paid to the following schemes:

1. Baptista's scheme in Baptista (1998) which forms the main thrust of the research work. Efforts were made to critique the scheme by analyzing its development and implementation and subjecting it to popular cryptanalytic attacks to reveal its weaknesses and possible areas of improvement.
2. Lawande's scheme in Lawande et al. (2005)

*Corresponding author. E-mail: folorunsolusegun@yahoo.com. Tel: +234-803-564-0707.

implemented logistic map model.
3. -Wong's scheme in Wong (2002) from which the idea of encrypting with look-up table (which we call tabu table) was drawn for enhancing the strength of the new scheme.

CHAOTIC SYSTEM

Chaos is one of the possible behaviours associated with evolution of non-linear physical systems and occurs for specific values of system parameters. The discovery of this apparently random behaviour ensuing out of deterministic systems, according to Alvarez et al. (2006) turned out to be quite revolutionary leading to many issues interconnecting stability theory, new geometrical features and new signature characterizing dynamical performance.

Characteristics of chaotic system

Systems which are basically non-linear and exhibiting apparently random behaviour for certain range of values of system parameters is said to be chaotic. In a peculiar manner, the solution or trajectories of the system are bounded within a region in the phase space. This unstable state has a strong dependence on the values of the parameters and on the way the system begins. Sensitivity to initial conditions, ergodicity and mixing are the cardinal properties of chaotic models which make them useful for encryption as noted in Moldovyan (2007).

Studying properties of chaotic model

In-depth understanding of the trajectory growth and behaviour of the chaotic function to be used as a model for encryption is essential in chaotic cryptography. For this purpose, some statistical tools can be used. Application of some of these tools to logistic map (our model in this research work) is described as follows:

Bifurcation diagram

The study of the trajectory growth of most chaotic systems shows an unsteady behaviour. For some parameter values, a chaotic system will be stable and as such disp-lay a periodic behaviour to parameter changes. For other parameter values, the system becomes unstable and is said to display a chaotic behaviour. Bifurcation diagram is used to study this property of chaotic systems (Figure 1).

Lyapunov exponent

Lyapunov exponents are used to determine whether the system is chaotic or not. If the system is chaotic, the difference between two trajectories with close initial condition will exponentially increase after a very short time. The difference is defined as

$$d_t = d_0 2^{\lambda t}$$

Where d_o = initial distance, d_t = distance at time t and λ = Lyapunov exponent.

Because d_t does not grow exponentially along the line, the expression is solved by averaging the points. The equation is defined as

$$\lambda = \frac{1}{t_n - t_0} \sum_{k=1}^{n} \log_2 \left(\frac{d_{tk}}{d_{tk-1}} \right)$$

Using this equation, the motion of the system is considered chaotic if $\lambda > 0$, quasi-periodic if $\lambda = 0$ and the system is in regular or periodic motion if $\lambda < 0$. Figure 2 shows variations in the lyapunov exponent of logistic map. It shows that logistic map becomes chaotic when $r > 3.57$.

Assessment of the existing schemes due to Baptista and Lawande

Baptista's scheme as illustrated in Baptista (1998) is based on a discrete time one-dimensional logistic map proposed by R.M May in 1976. The map represents an idealized ecological model for describing yearly variation in the population of insect species (Alligood, 1996). The population at $(n+1)^{th}$ year is mathematically related to that at the n^{th} year by the following map:

$$X_{n+1} = rx_n(1 - x_n)$$

where r = parameter.

In Baptista's scheme, iterates are generated using the above equation by choosing the parameter 'r' for chaotic regime and with initial condition $x_o \in [0, 1]$. A set of large number of these iterates [~60,000] is called a trajectory. Due to ergodic property, the interval (0,1) is visited frequently by the iterates. The density of such points is time invariant and Baptista's method of encryption is based on this feature. The scheme for encryption/de-cryption of a message uses the following steps:

Trajectory generation and mapping

Choosing the parameter $r \in [0, 4]$ (the chaotic region) and an initial condition $x_o \in [0,1]$, a sequence of points forming a trajectory is generated by iterating the logistic map:

$$X_{n+1} = rx_n(1 - x_n)$$

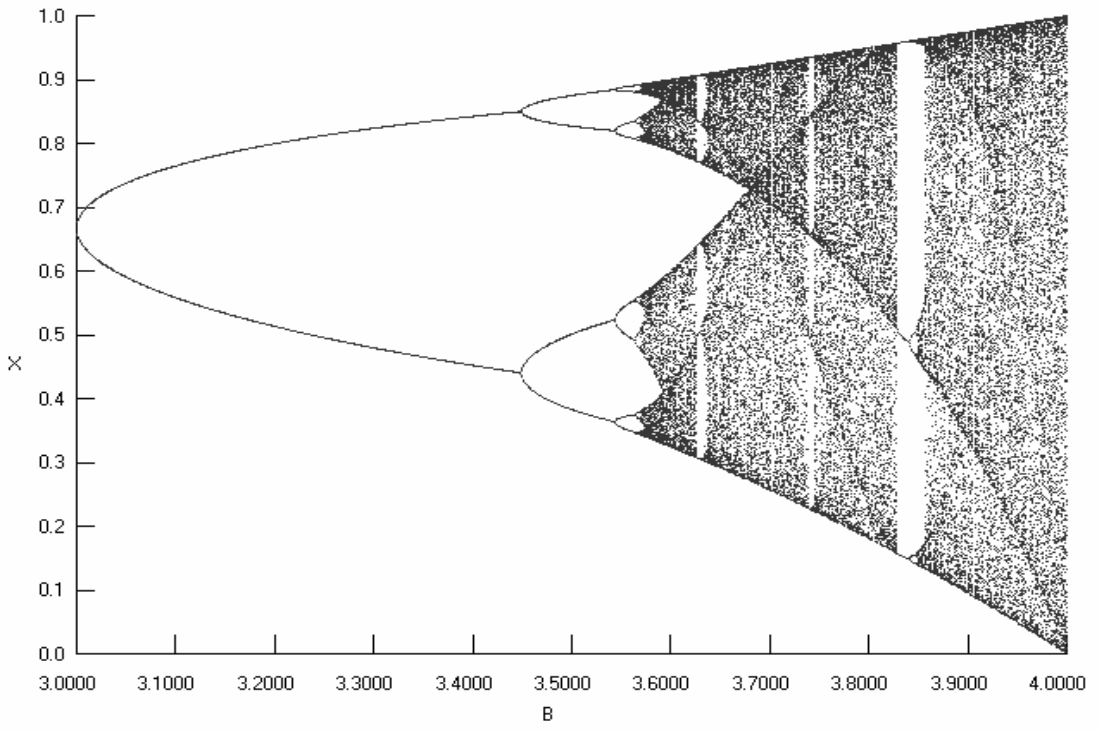

Figure 1. Bifurcation diagram of logistic map.

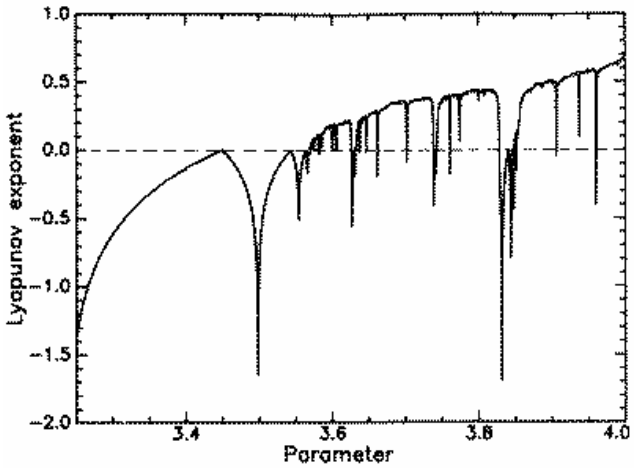

Figure 2. Diagram illustrating variations in lyapunov exponent of the logistic map: f(x) = rx(1 – x).

where $x_n \in (0,1)$.

An interval $[x_{min}, x_{max}]$ of the trajectory generated in step (1) is divided into S ≤ 256 sites.

$$\in = \frac{x_{max} - x_{min}}{s}$$

(Cells) each of size and to associated as typically shown in Figure 3. each of these sites, a byte

Xmin											Xmax
%	?	A	b	•	•	•	•	$	#	@	*
1	2	3	4	•	•	•	•	S-3	S-2	S-1	S

Figure 3. Division of logistic map Attractor into S sites.

or an ASCII character is For encrypting each character of a text, one finds the number of iterations necessary to reach the site belon-ging to that character.

The number of iterations is the cipher text representing the character. The process is repeated till the whole message is encrypted into a set of numbers. This forms the cipher text. Decryption is done by running the same algorithm with the same keys and the number of iterations equal to the integer values in the cipher text and by reverse mapping the site number into the character.

Analysis of Baptista's scheme

Suitable algorithms were developed for implementing Baptista's encryption and decryption models. The process of running algorithms for attacking the ciphers generated revealed some fundamental weaknesses inherent in the scheme.

Algorithm on Baptista's scheme

Step 1: Iterate 60,000 times to allow the model $x_{n+1} = r\ x_n$

(1 - x_n) settle down in chaos.

Step 2: Create book set. Here, 256 cell sites are created using an interval

$$i = \frac{x_{\max} - x_{\min}}{256}$$

where x_{max} and x_{min} are the boundary values. Attach an ASCII character to each cell site

Step 3: Get a character from the string of plaintext

Step 4: Encrypt the character. Here, choose a value for x_o between 0 and 1 and a value for r between 3.4 and 4.0. x and r are keys

Starting from initial value (x_o), the logistic map $X_{n+1} = rx_n(1-x_n)$ is iterated, until the iterate falls within the site allocated to the character. Store the iterate number (n) as the cipher representing the plaintext

Step 5: Check if the string from the plaintext is empty, if not go to Step 3 else, continue.

Step 6: Stop

Observations on the range of values specified for keys

During the implementation process, the response of the scheme was studied by fixing the value of x_o and varying the value of r. The results obtained in the process are contained in Table 1.

A close study of the bifurcation diagram (Figure 1) for logistic map revealed that at certain values of r ($3.4 \leq r < 3.57$), the map is still in its quasi-periodic region and it has not yet entered into its chaotic attractor. This explains the failure of the scheme to converge when the system parameter was chosen from within this region. The logistic map algorithm was run in MATLAB to generate the frequency plots of the trajectories for various values of r and for values x_o between 0 and 1. From these plots, we can deduce that it is necessary to redefine the range of valid points/values for encryption as contained in Table 2. In using Baptista's scheme for encryption, the parameters must be chosen within the ranges specified in this table for the scheme to be functional.

Lawande's variant scheme

A variant scheme was developed by Lawande et al. (2005). Though it is based on Baptista's model, a different idea is used to achieve one to many mapping. By this approach, the chaining effect of the original Baptista's scheme was overcome. A new key - η, is introduced thus enlarging the key space. The operation of the scheme is such that when the trajectory hits the site, a random number (k) is generated and compared with the preset η.

If k >η, then the iterate number is taken. Otherwise, the iteration is continued until the condition k > η is satisfied. The scheme can be implemented using the following algorithm:

Baptista with probability term (pre set η) – Lawande's Scheme

Step 1: Iterate 60,000 times to allow the model $X_{n+1} = rx_n(1-x_n)$ settle down in chaos. In the iterate generated, select x_{max} and x_{min}

Step 2: Create block set. Here, 256 cell sites are created using an interval

$$i = \frac{x_{\max} - x_{\min}}{256}$$

Where x_{max} and x_{min} are the boundary values. Attach an ASCII character to each cell site.

Step 3: Get a character from the string of plaintext

Step 4: Encrypt the character

Here, choose a value for x_o between 0 and 1, r between 3.40 and 4.00 and η between 0 and 1. x_o, r, and η are keys

Step 5: Starting from initial value x_o, the logistic map $x_{n+1} = rx_n (1 - x_n)$ is iterated, until the iterate falls within the site allocated to the character.

Step 6 : On hitting the site, generate a random number k

Check if $k \geq \eta$
If yes go to Step 8,
Otherwise, go to Step 7

Step 7: Continue iterating until the iterate falls within the site allocated to the character, go to Step 6.

Step 8: Store the iterate number (n) as the cipher representing the plaintext.

Step 9: Check if the string from the plaintext is empty, if yes, go to Step 10.
Else go to Step 3.

Step 10: Stop.

Table 1. Performance assessment of Baptista's encryption scheme.

System parameter r	Start value x_o	Volume of Plaintext (bytes)	Volume of cipher text (bytes)	Volume of recovered plaintext (bytes)	Time of encryption (s)	Time of decryption (s)
3.40	0.455	106	-	-	∞	∞
3.45	0.455	106	-	-	∞	∞
3.50	0.455	106	-	-	∞	∞
3.55	0.455	106	-	-	∞	∞
3.58	0.455	106	417	108	0.016	0.235
3.60	0.455	106	442	108	0.110	0.265
3.65	0.455	106	461	108	0.132	0.272
3.70	0.455	106	465	108	0.147	0.275
3.75	0.455	106	416	108	0.173	0.284
3.80	0.455	106	437	108	0.195	0.293
3.85	0.455	106	425	108	0.198	0.316
3.90	0.455	106	411	108	0.201	0.322
3.95	0.455	106	402	108	0.205	0.331
4.00	0.455	106	378	108	0.210	0.348

Table 2. Functionality assessment of Baptista's scheme.

System parameter r	Start value x_o
3.4 - 3.57	Invalid values for encryption
3.58 - 3.69	0.32 - 0.60, 0.79 - 0.90
3.70 - 3.79	0.26 - 0.92
3.80 - 3.89	0.18 - 0.95
3.90 - 3.99	0.10 - 0.97
4.00	0.10 - 1.00

Observation

It was seen that 97% of the occurrence of 'a' in the plaintext, is represented by the same cipher - 5162. The efficacy of probability factor η for achieving one-to-many mapping is evaluated by comparing the ciphers of ten ASCII sets (results are presented in Table 3). The assessment of the degree of variability was concluded by passing varying number of ASCII sets into the encryption scheme and computing the randomness coefficient for each case. The results obtained are illustrated in Figures 4 and 5 and presented in Table 4.

PROPOSED CIPHER SCHEME

Recognizing the shortcomings of Baptista's scheme and the weakness of Lawande's variant scheme, a new scheme is proposed. Based on Baptista's model, a unique idea is used to achieve one to many mapping. Here, each character in the plaintext is encrypted by iterating from the same x_o. However, at the point of hitting the cell sites, two parameters are used to determine whether the ciphering should be done or not.

Condition I

A random number is generated and it is compared with a preset coefficient η. The condition (k >η) is evaluated. If the condition is met, the scheme moves on to evaluate the second condition

Condition II

A tabu table is developed (which is an array of n consecutive ciphers). If condition I is met, the iterate number to be picked must not be in the tabu list - to avoid repetition as it occurs in Lawande's idea.

When the two conditions are met, the iterate number is taken as the cipher representing the plaintext. By this approach, the chaining effect of the original Baptista was overcome. A new key - η, is introduced thus enlarging the key space and making it more difficult to break by brute-force attack.

Design of architecture

An encryption system is made of two phases - the encryption phase and the decryption phase. In the encry-ption phase, the system accepts a message (plaintext) and applying appropriate algorithm and keys converts the message to an unintelligible form (cipher text). In the second phase, the inverse algorithm is applied with appropriate keys on the cipher text to obtain the original

Table 3. Functionality assessment for Lawande's scheme.

Coefficient η	Random coefficient α	Functionality
0.0	0	One-to-one mapping
0.1	0.00705	Successful one-to-many mapping
0.2	0.01899	"
0.3	0.03068	"
0.4	0.04214	"
0.5	0.06932	"
0.6	0.07150	"
0.7	0.09324	"
0.8	0.12231	"
0.9	0.16110	"
1.0	-	No encryption

Plaintext:

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaa

Cipher text:

Baptista:

234 1583 732 718 335 36 166 1355 86 620
158 165 233 418 22 1388 183 72 261 343
626 92 656 30 237 261 597 255 555 1129
406 76 1242 28 947 449 513 178 110 148
483 301 351 84 195 360 263 382 391 190

Lawande:

5162 5162 5162 5162 5162 5162 5162 5162 5162 5162
5162 5162 5162 5162 5162 5162 5162 5162 5162 5162
5162 5162 5162 5162 5162 5162 5162 5162 5162 5162
5162 5162 5162 5162 5162 5162 5162 5162 5162 5162
5162 5162 5162 5162 5162 5162 5162 5162 3127 4175

New Scheme:

282	591	2116	2062	1507	1215	269	2137	284	215
1826	1796	3970	5460	2090	5459	3291	2127	3936	9425
3903	1458	2373	5187	1746	7035	10023	256	292	7638
6039	10572	3900	3971	13924	4198	3273	11248	16148	2122
232	7865	3583	13044	3910	874	13676	5431	4242	1471

Recovered Plaintext:

aaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaa

Figure 4. Samples of redundant Plaintext-Cipher text-recovered Plaintext for the three schemes.

message (plaintext) back. In the design, a chaotic model - logistic map $X_{n+1} = rx_n(1-x_n)$ is used in building the algorithm. The keys are the start/initial value (x_o), system parameter r and the coefficient η.

Encryption engine: Baptista with tabu - table

Step 1: Iterate 60,000 times to allow the model $x_{n+1} = rx_n (1 - x_n)$ settle down in chaos

Here, choose a value for x_o, r from Table 2 and η from

Plaintext

```
The smaller the volume of the file
produced, the better the scheme.
```

Baptista's Scheme:

Cipher text

```
828   509   15    490   215   34    48    99    484 1059
630   402   298   576   217   343   16    2785  848 224
705   47    378   565   57    1327  110   222   902 1279
782   578   1333  847   88    444   569   505   523 808
1215  290   782   224   648   98    538   976   142 71
573   204   196   148   3743  797   17    235   75  1038
291   553   5     302   510   810   126
```

Recovered Plaintext

```
The smaller the volume of m_Îr¨¡ Â¨±ôÉ´üë
ý²Òòý(∏»Öu∏ ‰ ÓÐqÐÆ∏ ∏ isúþBš;ăø≈ăïç€&
```

Improved Scheme:

Cipher text

```
6289  150   8984  11377 17192 6572  5980  10198 2273  14781
484   1308  6243  6899  18760 8048  9298  6593  1993  6290
21456 1629  6874  9047  6875  9328  6898  13220 4715  539
996   8384  22935 3140  8385  1304  525   14707 9022  4424
9635  1067  9657  3450  11396 5603  9623  5614  11660 1049
10199 9046  19223 13186 9634  1053  3537  24433 5961  197
9656  11401 15371 25689 3139  1352  8087
```

Recovered Plaintext

```
The smaller the volum file produced,
the better the scheme.
```

Figure 5. Samples of Plaintext-Cipher text-recovered plaintext for two of the schemes – assessing the presence of chaining effect.

Table 4. Randomness coefficient table for Baptista's encryption scheme.

No.of ASCII Sets N	Randomness coefficient α		
	Baptista	Lawande	New scheme
2	0.09829	0.02835	0.17139
5	0.18772	0.06411	0.23256
10	0.26491	0.09324	0.34139
20	0.42166	0.14530	0.53470
30	0.48537	0.19324	0.78412

Table 3 (x_o, r, and η are keys).

Step 2: Create block set. Here, 256 cell sites are created using an interval

$$i = \frac{x_{\max} - x_{\min}}{256}$$

where x_{max} and x_{min} are the boundary values. Attach an ASCII character to each cell site

Step 3 : Create a tabu table an array of dimension A(I)

Step 4: Get a character from the string of plaintext

Step 5: Set I = 1, Encrypt the character

Step 6: Generating x_i
Starting from initial value (x_o), the logistic map $x_{n+1} = r_{xn}$ (1 - x_n) is iterated, until the iterate falls within the site allocated to the character.

Step 7: On hitting the site, generate a random number k

Check if $k \geq \eta$
If yes go to Step 9,
Otherwise, go to Step 8

Step 8: Continue iterating until the iterate falls within the site allocated to the character,
go to Step 6

Step 9: Is the iterate number n in the tabu table? If yes go to step 8 else, Step 10

Step 10: Store the iterate number (n) as the cipher representing the plaintext.

Step 11: If l > 1000, empty the tabu table else go to step 4

Step 12: Check if the string from the plaintext is empty, If yes, go to Step 13,
Else, Select the next character in the plaintext, Set l = l + 1, go to Step 6.

Step 13: Stop.

Decryption algorithm: Baptista with tabu - table

Step 1: Iterate 60,000 times to allow the model $X_{n+1} = rx_n(1-x_n)$ settle down in chaos
Here, supply the keys x_o, r, and η.

Step 2: Create block set. Here, 256 cell sites are created using an interval

$$i = \frac{x_{\max} - x_{\min}}{256}$$

Where x_{max} and x_{min} are the boundary values. Attach an ASCII character to each cell site.

Step 3: Get a character from the cipher file Ci.

Step 4: Decrypt the number (cipher code), Starting from initial value (X_o), the logistic map $X_{n+1} = rx_n(1-x_n)$ is iterated to x_{ci}. The character to which the site in which x_{ci} lies is noted.

Step 5: Store the character as the plaintext representing the cipher in a cipher file.

Step 6: Check if the cipher file is empty

If yes go to Step 7, Else, pick the next number, go to Step 4

Step 7: Stop.

On range specification

To avoid the limitations of the Baptista's scheme and the weakness associated with the use of probability term in Lawande's variant scheme, the ranges of operation of the newly proposed scheme are specified as in Tables 2 and 3 that is, System Parameter r: (3.58 - 4.0) and η : (0.0 – 0.9)

COMPARATIVE ASSESSMENT OF THE THREE SCHEMES

Further studies also revealed that the more effective the one to many mapping system is, the more chaotic and unpredictable the encryption engine becomes and the higher the strength of the scheme. Therefore, to evaluate the effectiveness of the mapping technique in the scheme, a randomness coefficient factor was developed. The factor is described thus:

Randomness coefficient

The randomness coefficient of degree n for a chaotic encryption scheme is given by:

$$\alpha_n = \frac{1}{256}\sum_{i=1}^{256}(d * \sigma(\alpha_i)^2)^{\frac{1}{2}}$$

Where σ (α_i) denotes the standard deviation of the vector α_i
α_i is a vector of d distinct cipher for a plaintext character c_i, $1 \leq i \leq 256$

The coefficient uses two probability measures to characterize the deviation and variation of the cipher produced by the given algorithm. While deviation is mea-sured by the standard deviation σ_i, the variation is dete-rmined by counting the distinct iterates produced by the algorithm for a single character. A measure of central ten-dency - the root-mean-square, is then used to return a representative for product of the deviation and variation on all the ASCII characters.

On strength

Based on randomness coefficient

A plaintext message containing N ASCII sets was developed

Table 5. Randomness coefficient/functionality versus coefficient η for Lawande's and improved scheme.

Coefficient η	Lawande's scheme		Improved scheme	
	Random Coeff. α	Functionality	Random coeff. α	Functionality
0.0	**0**	**One-to-one mapping**	**0.31617**	**Effective encryption**
0.1	0.07005	Successful one-to-many mapping	0.31486	"
0.2	0.08799	"	0.31366	"
0.3	0.10688		0.31179	"
0.4	0.12142	"	0.31073	"
0.5	0.14218	"	0.30929	"
0.6	0.16123	"	0.30833	"
0.7	0.19324	"	0.34139	"
0.8	0.22341	"	0.31222	"
0.9	0.27126	"	0.31437	"
1.0	-	No encryption	-	No encryption

Table 6. Volume of Cipher file generated and time of encryption using same plaintext message for the three schemes.

Scheme	Volume of cipher file (KB)	Time of encryption (126 KB Plaintext file) (s)
Baptista's scheme	437	0.046
Lawande's scheme: Baptista with probability term	452	0.089
New scheme: Baptista with tabu table	652	3.62

loped and supplied to Baptista's encryption engine. Cipher texts are generated for a number of ASCII sets and the program computes an average of the degree of variability between the cipher texts representing each of the characters in the ASCII sets. Table 4 contains the values of randomness coefficient α recorded against varying number of encrypted ASCII sets N. As presented in Table 4, the scheme demonstrates high degree of variation between ciphers obtained when the same plaintext is encrypted several times within a message. This is as a result of the effectiveness of the method used to achieve one to many mapping in Baptista's model and it is responsible for the strength of the scheme to various attacks.

Using highly redundant text file

This is as given in Figure 5.

Sensitivity to probability factor η

The randomness coefficient test conducted on Lawande's scheme shows that for low values of η (between 0.1 and 0.6), the randomness coefficient is very low (refer to Table 5). In essence, the cipher produced is similar to the product of a one-to-one mapping scheme which is highly vulnerable to chosen cipher text attack and frequency analysis attack.

However, for the improved scheme, the randomness coefficient test returned high values for all values of η (between 0.1 and 0.9). Hence the user can freely choose any value of η within this range as key for encryption to obtain a highly random cipher.

Volume and time of encryption of cipher file

The volume of the cipher file generated by a scheme is another criterion used for assessing the effectiveness and applicability of the scheme. The smaller the volume of the file produced, the better the scheme. Measurement of time taken for encryption/decryption processes and the volume of cipher file (as contained in Table 6) show that the improved scheme takes longer period and occupies larger space in the memory to be implemented. Thus it is not as effective as the other schemes.

Range specification

Analysis revealed that poor range specification is a major shortcoming of Baptista's scheme. With the range of (3.4 – 4.0) for r and (0 – 1) for x_o as specified by Baptista, experiments show that a user may not obtain successful encryption at all possible points in these ranges. Lawande's scheme also gives poor encryption for some value of η in the specified range (0 -1) as shown by

experiment. The improved encryption scheme is free from all these limitations as the functional intervals within these ranges have been identified and presented for users.

Presence of chaining effect

While Baptista's scheme suffers from this effect and it goes a long way in limiting its application in real life data processing systems, the improved scheme is free from chaining effect. If a character or segment of the cipher is corrupted or lost, the rest of the cipher text can be successfully recovered since the encryption of a plaintext character is not dependent on the preceding character.

General assessment of the schemes

Two notable defects of the scheme are:

1. Low speed of encryption and
2. Requirement of large memory space for cipher text

These defects are due to the fact that the encryption engine spends a lot of time searching the array of numbers which make up the tabu list. A solution is to reduce the array length. Presently, it is a set at 1,000. If it is reduced to 100 for example, the time of encryption will be shorter.

SUMMARY AND CONCLUSION

The basic goal of this research endeavour - to work out effective utilization of the ergodic properties of a chaotic model for data encryption using private key symmetric cryptographic model has been successfully achieved. The authors have been able to critique some existing schemes in the field of chaotic encryption and develop a functional and effective scheme void of the limitations identified in the existing ones. On implementation of this new scheme, the results of the performance evaluation exercise indicate that the scheme is practically effective for real-life encryption process. Furthermore, using chaotic models for building encryption schemes has proved to be simple, efficient and reliable option.

REFERENCES

Abir A, Safwan E, Wang Q, Calin V, Bassem B (2008). Comparative Study of 1-D Chaotic Generators for Digital Data Encryption. IAENG International J. Comput Sci.

Alligood KT, Sauer TD, Yorke JA (1996). Chaos: An Introduction to Dynamical Systems. Springer – Verlay New York Inc., New York NY 10010 USA.

Alvarez E, Fernadez A, Garcia P, Jimenez J, Marcano A (1999). New Approach to Chaotic Encryption. Phys, Lett. A., 263: 373-375.

Alvarez G, Fenandez L, Munoz J, Montoya F, Shujun L (2006). Security Analysis of a Communication System Based on the Synchronization of Different Order Systems. Chaos, Solitions and Fractals.

Alvarez G, Li S (2004). Breaking Network Security Based on Synchronization of Chaos. Comput. Communication, 27: 1689-1691.

Alvarez G, Montoya F, Romera M, Pastor G (2005). Cryptanalysing An Improved Security Modulated Chaotic Encryption Scheme Using Cipher-Test Absolute Value. Chaos, Solitons Fractals, 23: 1749-1756.

Alvarez G, Montoya F, Romera M, Pastor G (2004). Breaking Parameter Modulated Chaotic Secure Communication System. Chaos, Solitons Fractals, 21: 783-787.

Baptista MS (1998). Cryptography with Chaos. Phys. Lett. A, 240: 50 - 54.

Bose R, Amitabba B (1998). Implementation Symmetric Cryptography Using Chaos Functions. Indian Institute of Technology, Haz Khas, New Delhi.

Caroll TL, Pecora LM (1991). Synchronizing Chaotic Circuits. IEEE Trans. Circuit Syst., 38: 453 - 456.

Changsong Z, Lai CH (2000). Extracting Message Masked by Chaotic Signals of Time - Delay Systems. National University of Singapore.

Chee CY, Xu D, Bishop SR (2004). A Zero-Crossing Approach To Uncover The Mask By Chaoencryption With Periodic Modulation. Chaos Solitons Fractals, 21: 1129-1134.

Huang F, Guan ZH (2005). Cryptosystem Using Chaotic Keys. Chaos Solitons Fractals, 23: 851-855.

Kocarev L, Jakimoski G (2001). Logistic Map As A Block Encryption Algorithm. Phys. Lett. A, 289: 199-206.

Kwok HS, Wallace, Tang KS, Man KF (2004). Online Secure Chatting System using Discrete Chaotic Map. Int. J. Bifurcat. Chaos, 14 (1): 285-292.

Lawande QV, Ivan BR, Dhodapkar SD (2005). Chaos based Cryptography - A New Approach to Secure Communication. Base Newsletter p. 258.

Masuda N, Aihara K (2005). Cryptosystem with Discretized Chaotic Maps. IEEE Trans. Circuits Syst. I, (49): 851-855.

Moldovyan N (2007). Innovative Cryptography, Second Edition. Charles River Media, Boston, USA.

Solak E (2004). On the Security of a Chaos of Discrete - Time Chaotic Cryptosystems. Phys. Lett., 320: 389 - 395.

Tang S, Chen HF, Hwang SK, Liu JM (2002). Message Encoding and Decoding through Chaos Modulation in Chaotic Optical Communication. IEEEE Trans. Circuit Syst., I 49: 163-169.

Tsun - I Chin, The-Lu Liao (2005). Design of Secure Digital Communication System based on the Synchronization of Different Order Systems. Chaos, Solitons and Fractals.

Wong KW (2002). A Fast Chaotic Cryptographic Scheme with Dynamic Look-Up Table. Phys. Lett. A, 298: 238-242.

Wong KW, Ho SW, Yung CK (2003): A Chaotic Cryptography Scheme for Generating Short Ciphertext. Phys. Lett. A, 310: 67-73.

Yang T, Zidong W, Jian-an F (2009). Image Encryption Using Chaotic Coupled Map Lattice with Time-varying Delays. Communications in Nonlinear Science and Numerical Simulation, CNSNS 1303.

Zhang L, Liao X, Wang X (2005). An Image Encryption Approach based On Chaotic Maps. Chaos, Solitons Fractals, 24: 759-765.