Cryptographic construction using coupled map lattice as a diffusion model to enhanced security

Professors from DU...!

- ~~Cou~~ In Couple map lattice $\boxed{\text{(CML)}}$, every one-bit change in a pixel of plain image leads to a change in large number of pixels in the cipher image.
- CML model are more secured than 1-D chaos based encryptions
- uses secret key a $\boxed{\text{280-bit}}$ longer binary number.
- Image encryption ~~most~~ generally used in medical images.

older models reffered here, in this paper are :-

Hue et al → high speed scrambling and pixel adaptive diffusion process.
Cao et al → edge maps derived from a medical image.
Laiphrakpam → EIGamal encryption scheme (Improved version)
Ravichandran et al → coupling of logistic-tent and logisticsine system
Ravichandran et al → based on deoxyribo nucleic acid and chaotic maps.

- chaotic dynamical systems, coupled map lattice ~~provides~~ has been investigated as better diffusion model. CML provides the wide range of initial conditions and control parameters that further resulted in larger keyspace.
- CML is utilised into the proposed cryptographic Image encryption model as a diffusion model due to its superiority.

②

★ The design of coupled map lattice based image encryption algorithm

i) key generation.

A 280-bit long random binary secret key (k) is used to generate control parameters and initial conditions that are utilized in intertwining logistic map and coupled map lattice (CML).

The key is further divided in 35 block ($k_1, k_2, \ldots k_{35}$) of 8 bit size each. → alway verify from the paper [may have typo in writing]

$$k = k_1 k_2 k_3 k_4 \ldots k_{35} \quad (1)$$

check from internet?

$$\mu = 3.99 + \left[\left((k_2 + k_5) \oplus (k_1 \oplus k_2 \oplus \ldots k_{35})\right) \bmod 2\right] / 100 \quad (2)$$

$$\epsilon = \left(\left[(k_{24} + k_{19}) \oplus (k_1 \oplus k_2 \oplus \ldots k_{35})\right] / [k_8 + k_{21}]\right) \bmod 1$$

$$x_1 = \left[\left([k_{35} + k_{11}] \oplus [k_1 \oplus k_2 \oplus \ldots k_{35}]\right) / (k_{32} + k_{12})\right] \bmod 1 \quad (3)$$

(4)

$$x_2 = \left[\left([k_{30}] \oplus [k_1 \oplus k_2 \oplus \ldots k_{35}]\right) / (k_{20} + k_{15})\right] \bmod 1 \quad (5)$$

$$x_3 = \left[\left([k_{21} + k_{19}] \oplus [k \oplus k_2 \oplus \ldots k_{35}]\right) / (1 + k_{30})\right] \bmod 1 \quad (6)$$

$$y_1 = \left(\left[(k_{37} + k_{27}) \oplus (k_1 \oplus k_2 \oplus \ldots k_{35})\right] / [k_{14} + k_{16}]\right) \bmod 2 \quad (7)$$

$$y_2 = \left(\left[(k_9 + k_{22}) \oplus (k_1 \oplus k_2 \oplus \ldots k_{35})\right] / [k_{25} + k_{26}]\right) \bmod 2 \quad (8)$$

$$y_3 = \left(\left[(k_{34} + k_{33}) \oplus (k_1 \oplus k_2 \oplus \ldots k_{35})\right] / [1 + k_{28}]\right) \bmod 2.$$

word-plot ⇒ human interpretable

③

$Sf = k_1 \times k_{35} + (k_{21} \times k_{12}) \oplus k_9 + 113$ (10)

$\boxed{\oplus \text{ denotes bitwise XOR}}$

- CML initial conditions and control parameters totally depend on ~~the~~ key.
- Total no. of keys = 2^280 keys.
- Each key produces unique CML graph which is used in pixel value ~~in encryption~~ ~~mod~~ modification.

ii) Intertwining logistic map and coupled map lattice (CML)

Logistic map :- is a one-dimensional, discrete-time nonlinear system used to model chaos.

$$\boxed{x_{n+1} = r x_n (1 - x_n)}$$ for given specific values.

Intertwining logistic map :→ Inter + twin + logistic maps.
is formed by combining two or more logistic maps so that each one's evolution depends on the other's current states, creating mutual feedback.

e.g with two maps. (2D map's e.g.)

$$x_{n+1} = r_1 (1 - x_n) + \alpha y_n$$
$$y_{n+1} = r_2 (1 - y_n) + \beta x_n$$

Feedback

④

Intertwined 3D logistic map (given in the paper)

$$x_{n+1} = [\mu \times k_1 \times y_n \times (1-x_n) + z_n] \bmod 1$$

$$y_{n+1} = [\mu \times k_2 \times y_n + z_n \times (1 + x^2_{n+1})] \bmod 1$$

$$z_{n+1} = [\mu \times (y_{n+1} + x_{n+1} + k_3) \times \sin(z_n)] \bmod 1$$

where,

$0 < \mu \le 3.999$

$|k_1| > 34.9$

$|k_2| > 38.9$

$|k_3| > 36.7$

Note : output of one sequence (logistic map) depends upon the other two sequences.

advantages :

uses more number keys, results in larger key space, overcomes problem of blank and stable window, overcomes problem of uneven distribution of iterated sequences.

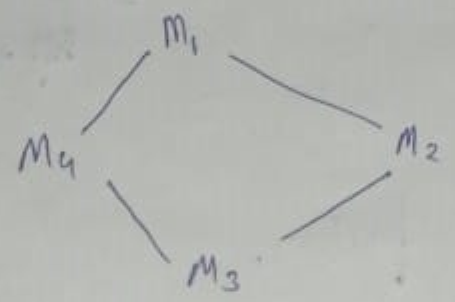
In the proposed model, pseudo random key stream generated from the intertwining logistic map are used in mixing process to change the image pixel values.

Hence mixing process makes the cipher image more reliant on intertwining logistic map.

Coupled map lattice (CML)

is basically a type chaotic function that utilizes logistic map to generate the chaotic sequence.

N→ [



CML is a lattice structure form of number of nodes where each node is itself an different logistic map.

~~The~~ Also, one's current value is dependent on neighbouring current value.]

advantages

- wide range of parameters
- strong chaotic behaviour
- less periodic window
- better pseudo random chaotic sequences
- more secured the 1-D chaotic values.
- substitutes the chaotic sequence to resist the statistic and differential attacks because Mutual Information for the chaotic sequence b/w lattices is not zero.

limitations:

Number of lattices play a significant role in image encryption.

A. According to paper, given below is a 2-D CML :-

$$x_{n+1}(k) = (1-\epsilon) f(x_n(k)) + \frac{\epsilon}{2}\left[f(x_n(k-1)) + f(x_n(k+1))\right]$$

left node right node

$$f(x) = 1 - \mu x^2$$

Here, $f(x)$ is a mapping function.

μ : constant , ranges btw 0 and 2.

ϵ : coupling coefficient , ranges btw 0 and 1.

for $\mu = 1.9$ and $\epsilon = 0.09$ CML shows chaotic behaviour.

iii) Mixing [easier to understand by code]

In the proposed mixing process, pixel values of the plain image are modified based on the pseudo random generated key stream using intertwining logistic maps (3D Intertwined here).

$$\boxed{P'_{i+1} = P_i \oplus RNG_i}$$

[given, $P_{i+1} = P_i \oplus RNG_i$ sequential XORs]

Pixel value [Red, Green, Blue] ↕ XOR ↕ [X, Y, Z of 3D Intertwined logistic map]

Step 1. XOR pixel value with logistic map value chaotic
Step 2. Column shuffle
Step 3 Row shuffle

NOTE :- mixing used to reduce correlation of pixel (neighbouring pixels)

Shuffling process

Used to break vertical and horizontal relationships in Xored matrix.

Let Xored matrix,

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix} \end{array}$$

column - shuffling

generate chaotic matrix C,

$$\text{let } C = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0.42 & 0.75 & 0.18 & 0.56 \\ 0.93 & 0.11 & 0.60 & 0.33 \\ 0.29 & 0.88 & 0.48 & 0.71 \\ 0.15 & 0.66 & 0.24 & 0.80 \end{bmatrix} \end{array}$$

sorted index

map accordingly

Column-wise sorting.

column	sorted (ascending)	Index
0.42, 0.93, 0.29, 0.15 →	0.15, 0.29, 0.42, 0.93 →	[3 2 0 1]
0.75, 0.11, 0.88, 0.66 →	0.11, 0.66, 0.75, 0.88 →	[1 3 0 2]

$$\text{So, } I_c = \begin{bmatrix} 3 & 1 & 0 & 1 \\ 2 & 3 & 3 & 0 \\ 0 & 0 & 2 & 2 \\ 1 & 2 & 1 & 3 \end{bmatrix}$$

each column of Is is vertical permutation for that column.

Column-wise shuffled P' =

$$
\begin{array}{c}
\begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\
\begin{bmatrix}
13 & 6 & 3 & 8 \\
9 & 14 & 15 & 4 \\
1 & 2 & 11 & 12 \\
5 & 10 & 17 & 16
\end{bmatrix}
\end{array}
$$

Row shuffling

Make a new or reuse the chaotic matrix list.

$$
C' = \begin{array}{c}
\begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\
\begin{bmatrix}
0.52 & 0.21 & 0.77 & 0.66 \\
0.48 & 0.10 & 0.93 & 0.35 \\
0.62 & 0.55 & 0.15 & 0.88 \\
0.14 & 0.40 & 0.81 & 0.27
\end{bmatrix}
\end{array}
$$

Rows	Sorted	Indexes
(0.52, 0.21, 0.77, 0.66)	(0.21, 0.52, 0.66, 0.77)	[1, 0, 3, 2]
(0.48, 0.10, 0.93, 0.35)	(0.10, 0.35, 0.48, 0.93)	[1, 3, 0, 2]

similarly for other rows as well

Index matrix for row-wise shuffle

$$
If = \begin{bmatrix}
1 & 0 & 3 & 2 \\
1 & 3 & 0 & 2 \\
2 & 1 & 0 & 3 \\
0 & 3 & 1 & 2
\end{bmatrix}
$$

Using row-index matrix try to shuffle alread column-wise shuffled matrix, let P''

$$\text{Row-wise shuffled } P'' = \begin{bmatrix} 6 & 13 & 8 & 3 \\ 14 & 4 & 9 & 15 \\ 11 & 2 & 1 & 12 \\ 5 & 16 & 10 & 7 \end{bmatrix}$$

iv) Confusion

Confusion is a process in which each part of the ciphertext is made dependent not only on plain image but also on the several part of secret key. It not only modify the image pixel values but also makes more complex relationship between plain and cipher image.

Confusion is used to prevent from "differential attacks".

$$\boxed{C_{i+1} = C_{i-1} \oplus k_i \oplus C_i \oplus ILM_i}$$