CrownCipher: A Queenly approach to Image Encryption

AJAY KUMAR – 125003017

GNANAPRIYA – 125003084

Dr. S. Priya, AP – III, SoC

Base Paper Details

- Iqbal, N. Image Encryption using Queen, Multimedia Tools and applications (2023)
- https://doi.org/10.1007/s11042-023-15674-6
- SCI – E indexed (2023)

PROBLEM STATEMENT

Traditional cryptographic techniques cannot be used to encrypt the digital images due to their different characteristics like high redundancy, large volume and strong inter-pixel relation.

Some techniques include low dimension chaotic maps which does not provide much randomness and has uneven distribution of sequences.

Schemes using King and knight pieces does not produce much scrambling effect. There is requirement to develop a cryptographic algorithm with sufficient plaintext sensitivity and more scrambling effects.

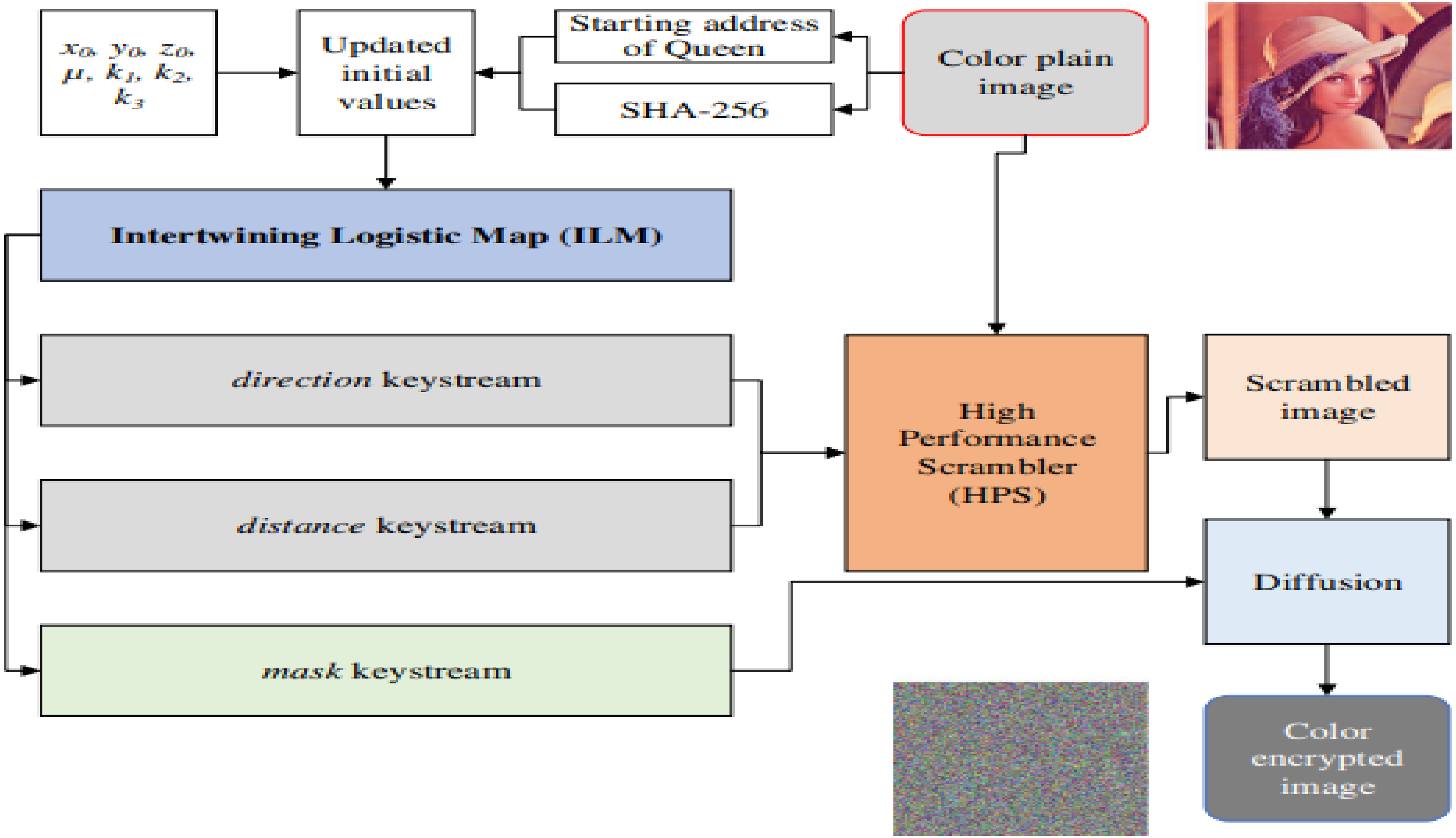
LITERATURE SURVEY

Year	Author	Title	Proposed Technique	Drawbacks
2016	Hua Z	Image encryption using 2D Logistic-adjusted-Sine map.	Proposes a new 2D chaotic map called 2D-LASM. Logistic map to adjust the input of the sine map and then extends its phase plane from 1D to 2D.	Usage of low-dimension chaotic maps.
2017	Pak C	A new color image encryption using combination of the 1D chaotic map	A method of making a simple and effective chaotic system by using a difference of the output sequences of two same existing one-dimension (1D) chaotic maps.	Developed by idea of confusion and diffusion but cryptanalyzed by different attacks.
2017	Xiaoyong J	Image encryption and compression based on the generalized knight’s tour, discrete cosine transform and chaotic maps.	The generalized knight’s tour algorithm is utilized to scramble the pixels while the data correlation preserved. The chaotic system is used to generate a pseudorandom permutation to encrypt the part of coefficients from discrete cosine transform for diffusion.	Limited scrambling effect of pixels due to Knight moving rules. Vulnerable to correlation attacks.

LITERATURE SURVEY

Year	Author	Title	Proposed Technique	Drawbacks
2016	Parvin Z	A new secure and sensitive image encryption scheme based on new substitution with chaotic function	In proposed scheme, two chaotic functions and logical operator xor are used. Image encryption process includes substitution of pixels and permutation.	High redundancy, large volume and strong inter-pixel relation.
2014	Boriga R	A new hyper chaotic map and its application in an image encryption scheme	The proposed map is then used in a new image encryption scheme: a diffusion stage, in which the pixels of the plain image are shuffled using a random permutation generated with a new algorithm, and a confusion stage, in which the pixels are modified with a XOR–scheme based on the proposed map.	The image ciphers based on higher dimension chaotic systems are difficult to implement and are less efficient.
2010	Wang XY	A chaotic image encryption algorithm based on perceptron model	Based on the high-dimension Lorenz chaotic system and perceptron model within a neural network, a chaotic image encryption system with a perceptron model is proposed.	Prone to chosen plaintext and known plaintext attacks.

WORKFLOW



$x_0, y_0, z_0, \mu, k_1, k_2, k_3$

Updated initial values

Starting address of Queen

SHA-256

Color plain image

Intertwining Logistic Map (ILM)

direction keystream

distance keystream

mask keystream

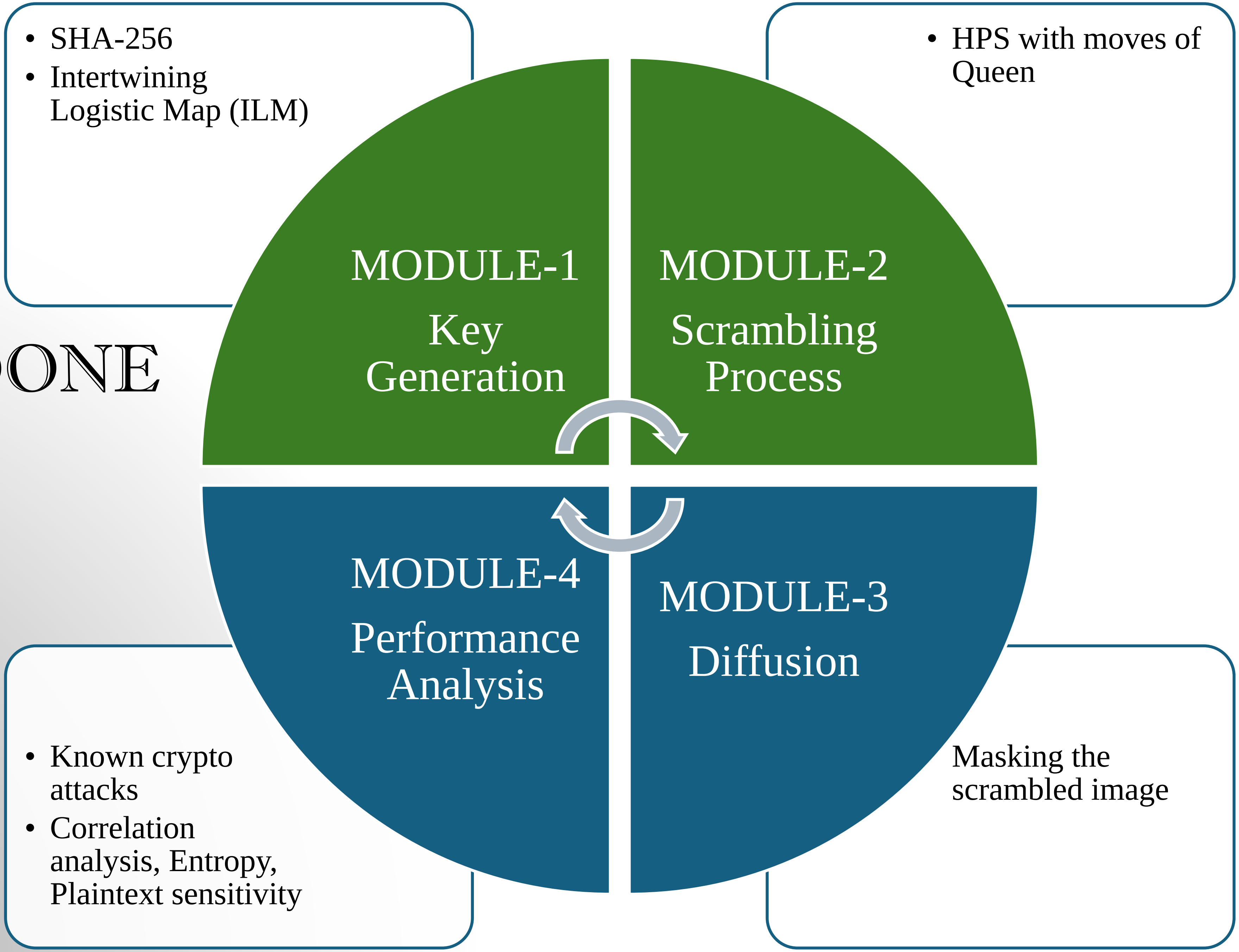
High Performance Scrambler (HPS)

Scrambled image

Diffusion

Color encrypted image

WORK DONE



MODULE-1
Key Generation

- SHA-256
- Intertwining Logistic Map (ILM)

MODULE-2
Scrambling Process

- HPS with moves of Queen

MODULE-3
Diffusion

Masking the scrambled image

MODULE-4
Performance Analysis

- Known crypto attacks
- Correlation analysis, Entropy, Plaintext sensitivity

KEY GENERATION

SHA256 Function

- Generating 256-bit Initial key from the input plain image which is further divided into thirty two 8-bit sub keys.

$$Key = key_1, key_2, ..., key_{32}.$$

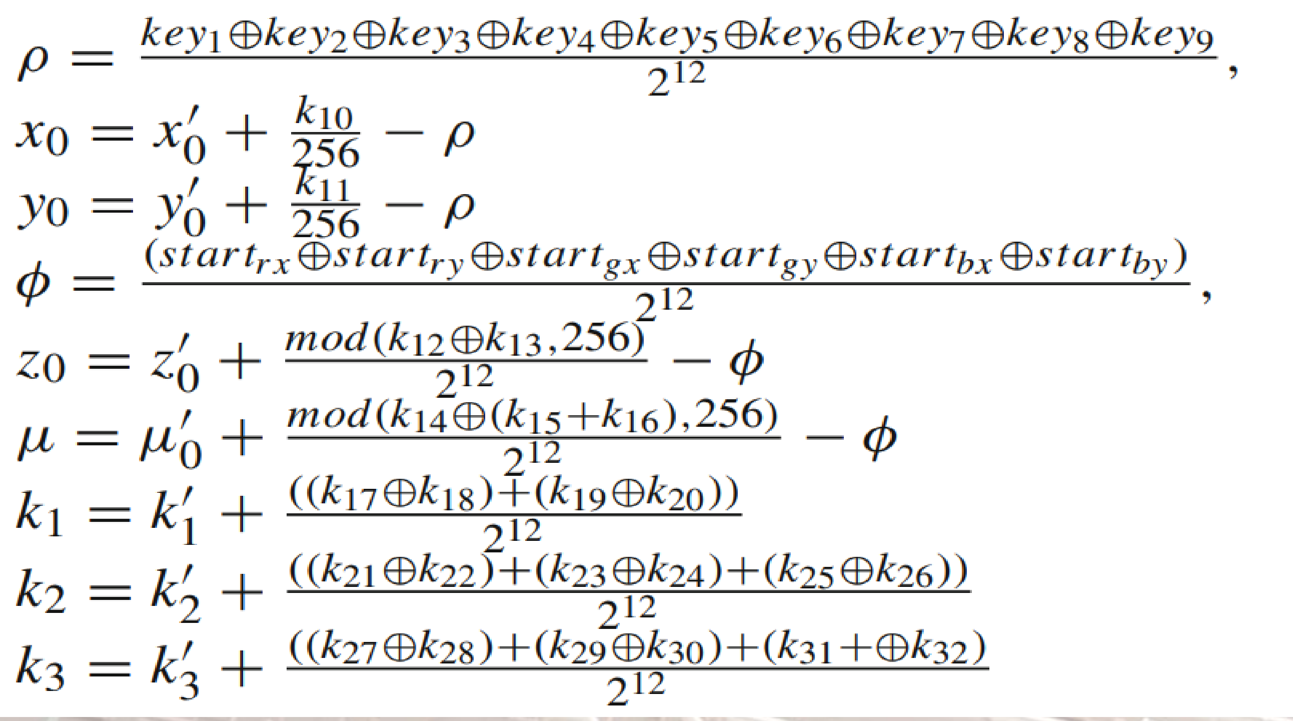
Generating secret keys and calculating starting position of Queen

$$\begin{aligned}
start_{rx} &= red(x_1, y_1) + 1 \\
start_{ry} &= red(x_2, y_2) + 1 \\
start_{gx} &= green(x_3, y_3) + 1 \\
start_{gy} &= green(x_4, y_4) + 1 \\
start_{bx} &= blue(x_5, y_5) + 1 \\
start_{by} &= blue(x_6, y_6) + 1
\end{aligned}$$

KEY GENERATION

Initialising the Initialization vector ($0 < x0, y0, z0 < 1,\ 0 < \mu < 3.999, k1 > 33.5, k2 > 37.9, k3 > 35.7$)

Updating the initialization vector ($x0, y0, z0, \mu, k1, k2, k3$)



$$\rho = \frac{key_1 \oplus key_2 \oplus key_3 \oplus key_4 \oplus key_5 \oplus key_6 \oplus key_7 \oplus key_8 \oplus key_9}{2^{12}},$$

$$x_0 = x_0' + \frac{k_{10}}{256} - \rho$$

$$y_0 = y_0' + \frac{k_{11}}{256} - \rho$$

$$\phi = \frac{(start_{rx} \oplus start_{ry} \oplus start_{gx} \oplus start_{gy} \oplus start_{bx} \oplus start_{by})}{2^{12}},$$

$$z_0 = z_0' + \frac{mod(k_{12} \oplus k_{13}, 256)}{2^{12}} - \phi$$

$$\mu = \mu_0' + \frac{mod(k_{14} \oplus (k_{15} + k_{16}), 256)}{2^{12}} - \phi$$

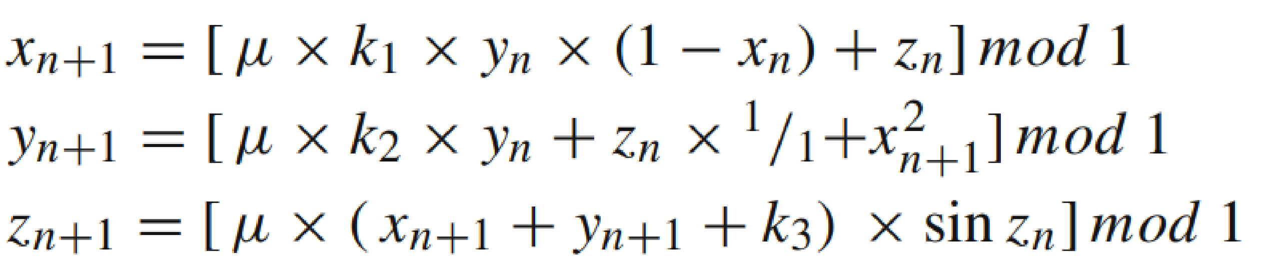
$$k_1 = k_1' + \frac{((k_{17} \oplus k_{18}) + (k_{19} \oplus k_{20}))}{2^{12}}$$

$$k_2 = k_2' + \frac{((k_{21} \oplus k_{22}) + (k_{23} \oplus k_{24}) + (k_{25} \oplus k_{26}))}{2^{12}}$$

$$k_3 = k_3' + \frac{((k_{27} \oplus k_{28}) + (k_{29} \oplus k_{30}) + (k_{31} + \oplus k_{32})}{2^{12}}$$

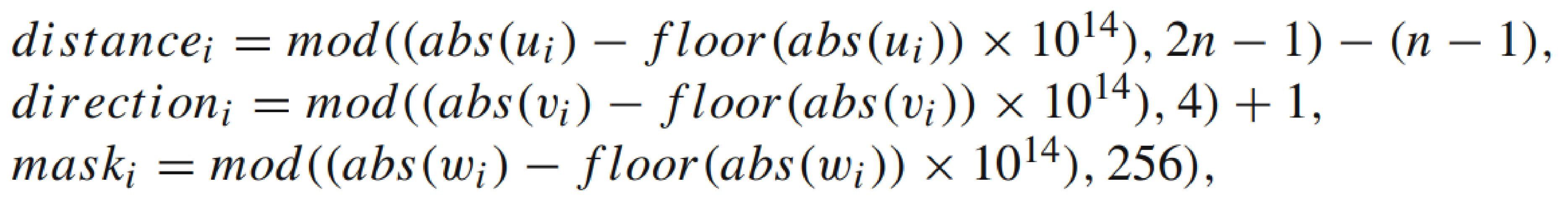
KEY GENERATION

Constructing three chaotic sequences (Intertwining Logistic Map)



$$x_{n+1} = [\,\mu \times k_1 \times y_n \times (1 - x_n) + z_n]\, mod\ 1$$
$$y_{n+1} = [\,\mu \times k_2 \times y_n + z_n \times {}^{1}/_{1+x_{n+1}^{2}}]\, mod\ 1$$
$$z_{n+1} = [\,\mu \times (\,x_{n+1} + y_{n+1} + k_3)\ \times \sin z_n]\, mod\ 1$$

Calculating *distance*, *direction* and *mask* sequences

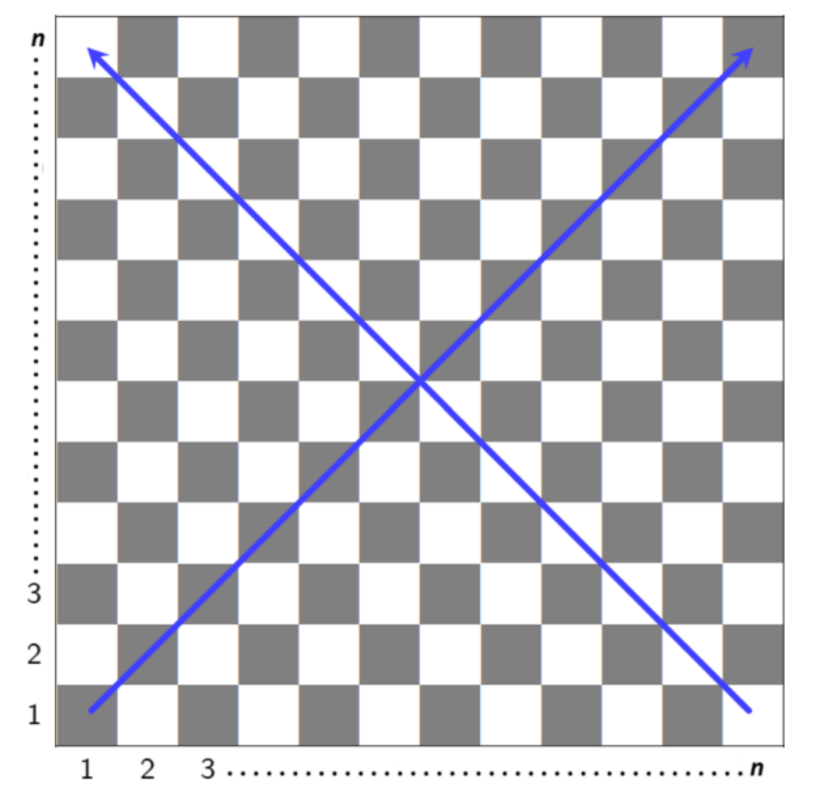


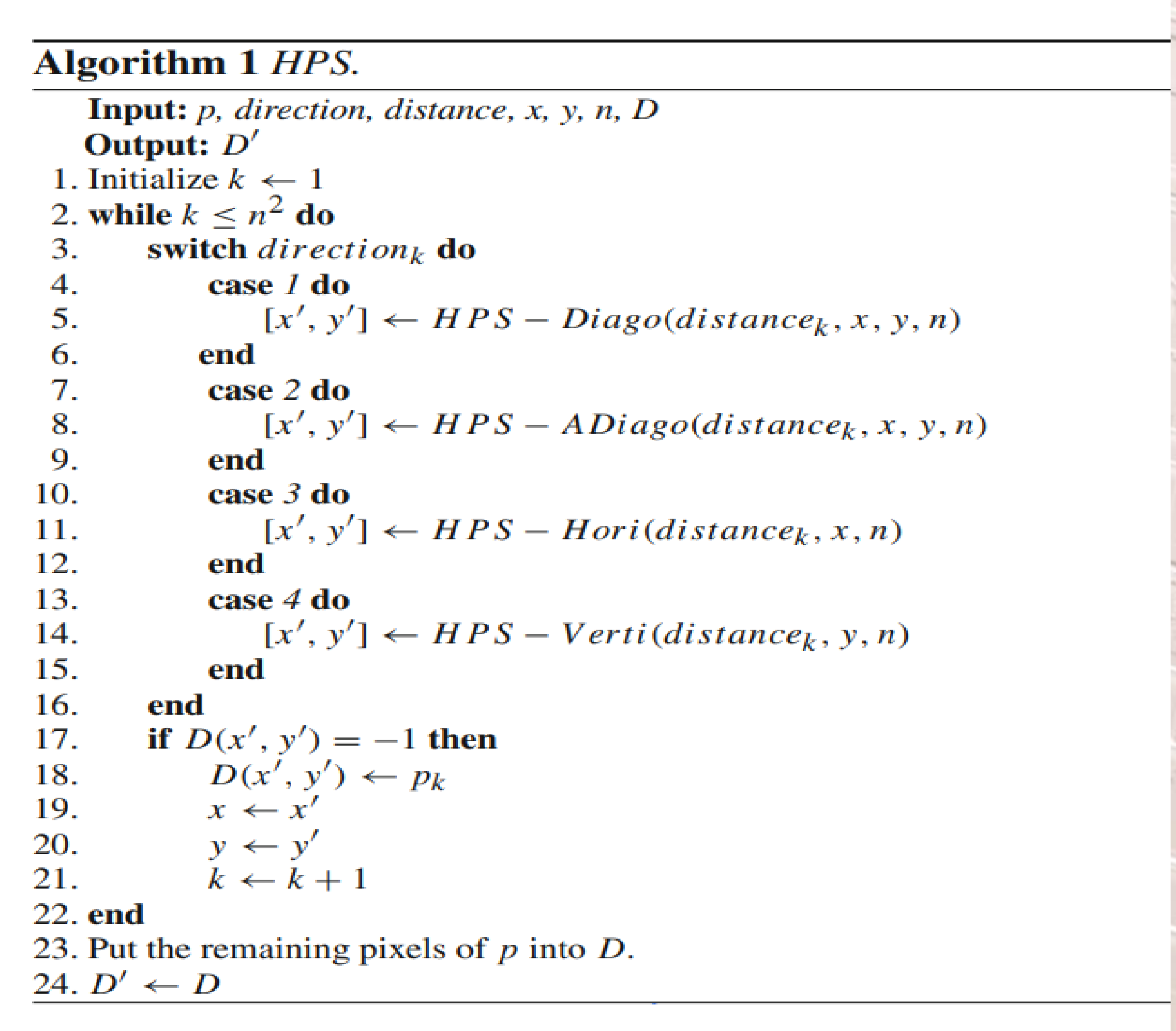
$$distance_i = mod((abs(u_i) - floor(abs(u_i)) \times 10^{14}), 2n - 1) - (n - 1),$$
$$direction_i = mod((abs(v_i) - floor(abs(v_i)) \times 10^{14}), 4) + 1,$$
$$mask_i = mod((abs(w_i) - floor(abs(w_i)) \times 10^{14}), 256),$$

SCRAMBLING PROCESS

Splitting the input plain image into three channels (*red*, *green* and *blue*)

High Performance Scrambler (HPS)





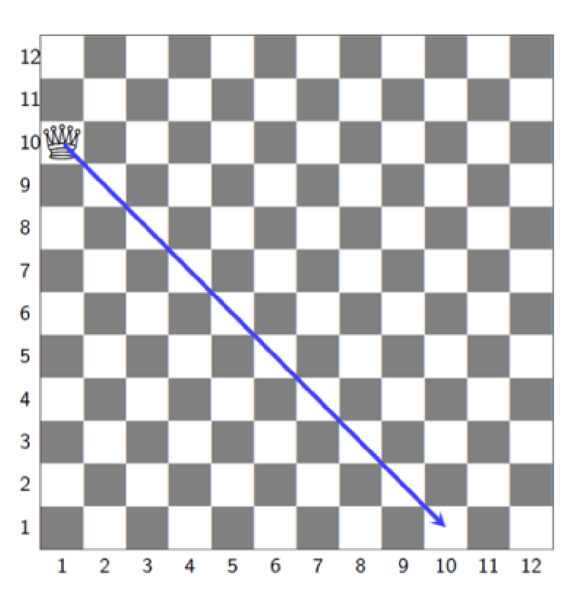
Algorithm 1 *HPS.*

```
Input: $p$, $direction$, $distance$, $x$, $y$, $n$, $D$
Output: $D'$
Initialize $k \leftarrow 1$
while $k \leq n^2$ do
    switch $direction_k$ do
        case 1 do
            $[x', y'] \leftarrow HPS - Diago(distance_k, x, y, n)$
        end
        case 2 do
            $[x', y'] \leftarrow HPS - ADiago(distance_k, x, y, n)$
        end
        case 3 do
            $[x', y'] \leftarrow HPS - Hori(distance_k, x, n)$
        end
        case 4 do
            $[x', y'] \leftarrow HPS - Verti(distance_k, y, n)$
        end
    end
    if $D(x', y') = -1$ then
        $D(x', y') \leftarrow p_k$
        $x \leftarrow x'$
        $y \leftarrow y'$
        $k \leftarrow k + 1$
end
Put the remaining pixels of $p$ into $D$.
$D' \leftarrow D$
```

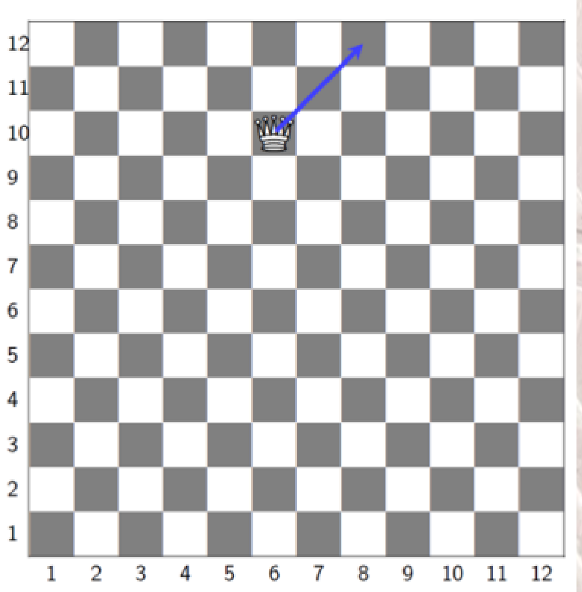
SCRAMBLING PROCESS

High Performance Scrambler (HPS)

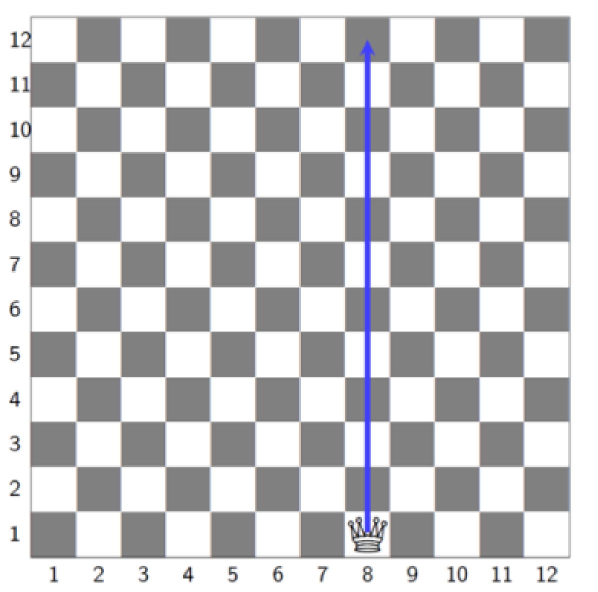
$$\begin{aligned}
red_1 &= HPS(red, \{direction_i\}_{i=1}^{n^2}, \{distance_i\}_{i=1}^{n^2}, start_{rx}, start_{ry}, n, D),\\
green_1 &= HPS(green, \{direction_i\}_{i=n^2+1}^{2n^2}, \{distance_i\}_{i=n^2+1}^{2n^2}, start_{gx},\\
&\qquad start_{gy}, n, D),\\
blue_1 &= HPS(blue, \{direction_i\}_{i=2n^2+1}^{3n^2}, \{distance_i\}_{i=2n^2+1}^{3n^2}, start_{bx},\\
&\qquad start_{by}, n, D)
\end{aligned}$$



[(1, 10), (10, 1), -9]

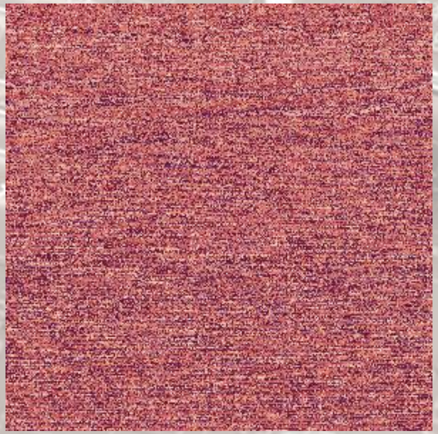


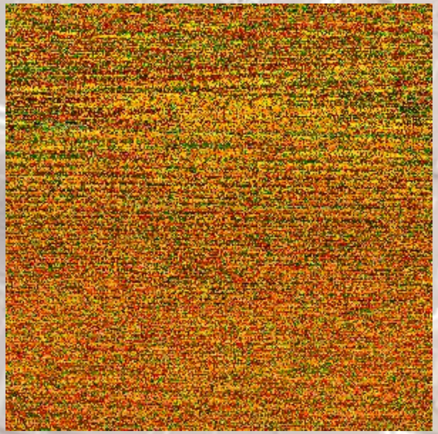
[(6, 10), (8, 12), 6] (Circular)

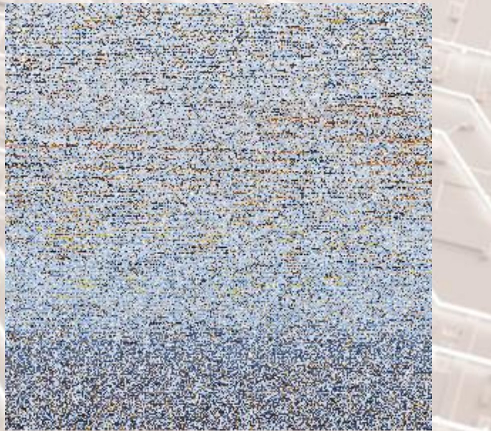


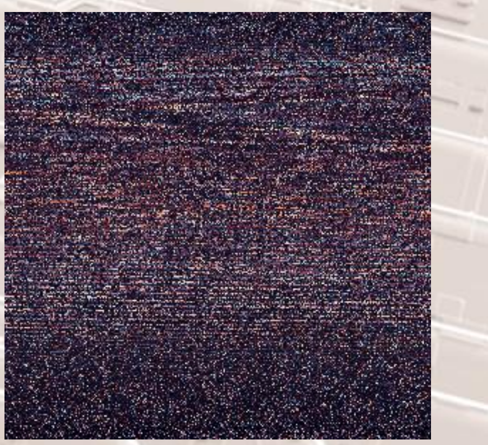
[(8, 1), (8, 12), 11]

SAMPLE OUTPUT

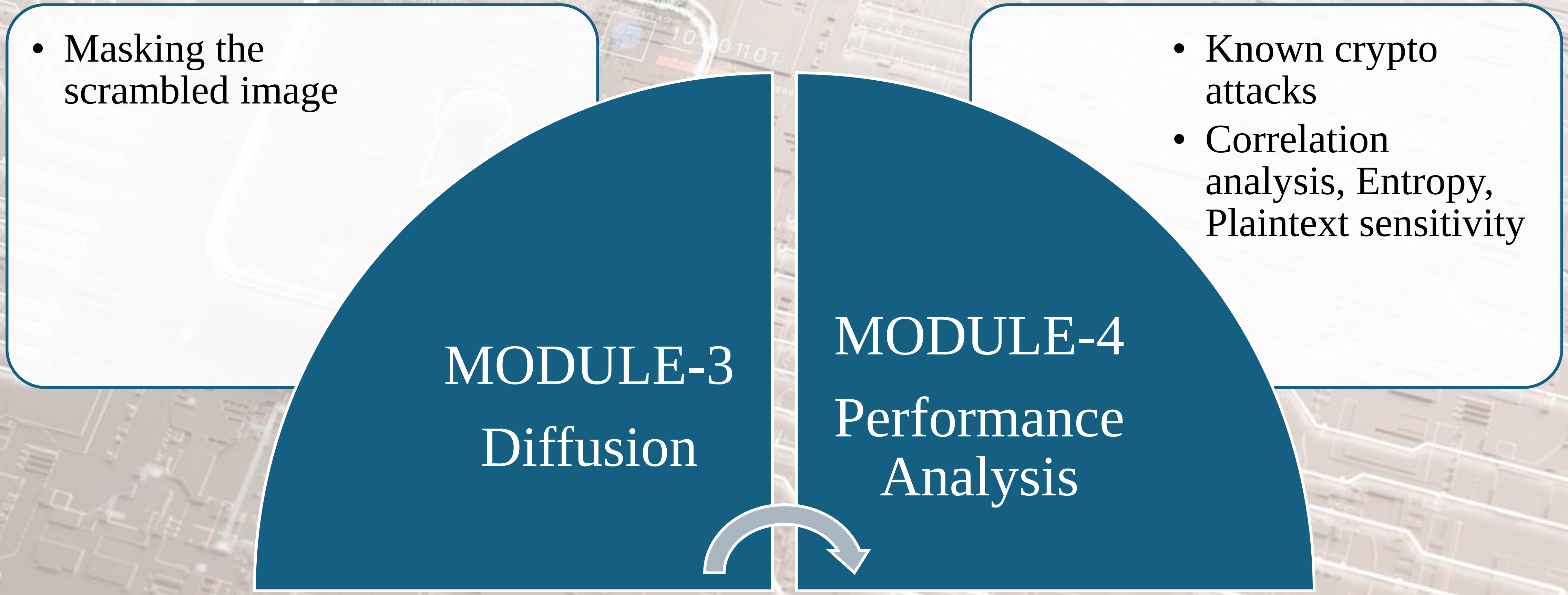








PENDING WORKS



- Masking the scrambled image

MODULE-3

Diffusion

MODULE-4

Performance Analysis

- Known crypto attacks
- Correlation analysis, Entropy, Plaintext sensitivity

REFERENCES

Hua Z, Zhou Y (2016) Image encryption using 2D Logistic-adjusted-Sine map. Inform Sciences 339: 237–253

Xiaoyong J, Sen B, Guibin Z, Bing Y (2017) Image encryption and compression based on the generalized knight’s tour, discrete cosine transform and chaotic maps. Multimed Tools Appl 76(10):12965–12979

Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. Signal Process 138:129–137

Wang XY, Yang L, Liu R, Kadir A (2010) A chaotic image encryption algorithm based on perceptron model. Nonlinear dynam 62(3):615–621

Boriga R, D˘asc˘alescu AC, Priescu I (2014) A new hyperchaotic map and its application in an image encryption scheme. Signal Process-Image 29(8):887–901

Parvin Z, Seyedarabi H, Shamsi M (2016) A new secure and sensitive image encryption scheme based on new substitution with chaotic function. Multimedia Tools Appl 75:10631–10648

THANK YOU