Soft Computing
https://doi.org/10.1007/s00500-023-08493-2

FOUNDATION, ALGEBRAIC, AND ANALYTICAL METHODS IN SOFT COMPUTING

# Highly secured and quickest image encryption algorithm based on trigonometric chaotic map and S-box

Ronnason Chinram[1] · Mahwish Bano[2] · Umair Habib[2] · Pattarawan Singavananda[3]

Accepted: 9 May 2023


**Abstract**
The purpose of this research is to develop a highly secured non-breakable fastest cryptosystem. A significant number of image encryption plans have been proposed during the past years. By far, most such plans arrive at a high-security level; be that as it may, their moderate velocities due to their complex phenomenon make them of no utilization progressively applications. Motivated by this, we propose another proficient and quick image encryption plan subject to the trigonometric turbulent guide. In contrast with most current plans, we utilize this basic map to create just a couple of arbitrary rows and columns in the form of S-boxes. Besides, to, moreover, accelerate, we raise the handling unit from the pixel level to the line/segment level. Security of the new plan is acquired through a replacement stage organization, where we implemented around the shift of lines and segments to break the strong relation between adjoining pixels and non-repeating sequences. By then, we join the Exclusive-OR operation with modulo capacity to cover the pixel esteems and avoid any spilling of information. High-security tests and reenactment examinations have been done to display that the plan is extremely safe and particularly speedy for continuous picture preparation at 80 fps (frames per second). The present research has developed a cryptosystem based on Exclusive-OR with S-box (Substitution Box) and trigonometric chaotic map (TCM) of image matrices. High security is achieved due to the non-repeating sequence of the TCM. Earlier, the author has already presented the efficacy of the TCM combined with the S-Boxes.

**Keywords** Encryption · Image encryption · S-box · Trigonometric chaotic map · XOR

## 1 Introduction

The speedy improvement in interactive media innovation and PC networks notwithstanding the expanded use of cloud-based capacity and huge information requires techniques to ensure individuals' private and secret information (Abu-Amara 2018). Simultaneously, the pre-owned insurance strategy ought to be exceptionally secure without compromising the framework's usefulness and ease of use to comfort clients (Panityakul et al. 2022). Picture encryption is one of the ordinarily utilized and compelling techniques to ensure pictures during capacity and transmission (Thinnukool et al. 2021). Conventional encryption techniques are not reasonable to encode pictures due to picture-inborn qualities like the relationship between picture pixels, low affectability to information change, and information repetition (Agarwal 2018). Turbulent guides hold alluring qualities, for example, unsteadiness of framework circle, basic execution, high affectability to a little change

✉ Pattarawan Singavananda
pattarawan.pe@skru.ac.th

Ronnason Chinram
ronnason.c@psu.ac.th

Mahwish Bano
mahwish@mail.au.edu.pk

Umair Habib
191764@students.au.edu.pk

[1] Division of Computational Science, Faculty of Science, Prince of Songkla University, Hat Yai, Songkhla 90110, Thailand

[2] Department of Mathematics, Air University, Islamabad 44000, Pakistan

[3] Program in Mathematics, Faculty of Science and Technology, Songkhla Rajabhat University, Songkhla 90000, Thailand

Published online: 16 June 2023

in starting condition and control boundaries, and pseudo-random (Bano et al. 2020). Distinctive turbulent guides were accounted for in the writing like convex sinusoidal map (Bano et al. 2017), parameter-varying baker map (Lawnik 2017), cross a chaotic map (Khan et al. 2019), generalized sine map (Sheela et al. 2017), combined sine and tent map (Paar 2014), generalized logistic map (Jin et al. 2019), and a few others (Guanghui et al. 2014). Each proposed turbulent guide enjoys its benefits and hindrances (Abu-Amara and Abdel-Qader 2013) as far as encryption time, security, and intricacy (Bano et al. 2017).

The strategic guide (Liu et al. 2018), quite possibly the most normally utilized tumultuous guide, has a little key space making it not immune against beast power assaults, doesn't give uniform dispersion of the iterative variable, and has an unsteady worth of Lyapunov exponent (Bano et al. 2016a). It was tracked down that the vast majority of the turbulent cryptosystems have deficient heartiness and security (Liu and Miao 2017). Another work detailed that the logistic guide, Mandelbrot map, and symmetric tent guide hold a huge arrangement of weaknesses (Bano et al. 2016b).

The paper is organized as follows. Section 1.1 and 1.2 describes the trigonometric chaotic map and its properties. Section 1.3 and 1.4 discusses the Galois field and related terms. Section 2 describes different mechanisms for the construction of S-Boxes using TCM and Galois field. Section 3 presents the proposed image encryption method. Section 4 discusses experimental results. Conclusions are presented in Sect. 5.

### 1.1 Trigonometric chaotic map

Equation (1) shows the proposed TCM.

$$w_{n+1} = \begin{cases} \alpha w_n \left[\sin\left\{\frac{\pi}{2} w_n\right\} + \cos\left\{\frac{\pi}{2} w_n\right\}\right] 0 \le w_n \le 0.5 \\ \alpha[1 - w_n]\left[\sin\left\{\frac{\pi}{2}(1 - w_n)\right\}\right. \\ \quad \left. + \cos\left\{\frac{\pi}{2}(1 - w_n)\right\}\right] 0.5 < w_n \le 1 \end{cases} \tag{1}$$

where the recurrence relation function, $w_{n+1} \in [0, 1]$, $w_0$ is the starting value and $\alpha$ is the control parameter.

### 1.2 Analysis of TCM properties

The characteristics of the trigonometric turbulent guide are investigated. The properties like chaotic behavior, s-unimodality, sensitivity to the initial condition, and uncertainty are investigated. Figure 1 displays the iteration function of the trigonometric turbulent guide. By examining the picture, we can without much of a stretch see that the cycle work starts from zero and continues to increment till it achieves the pinnacle worth of 1 and afterward begins

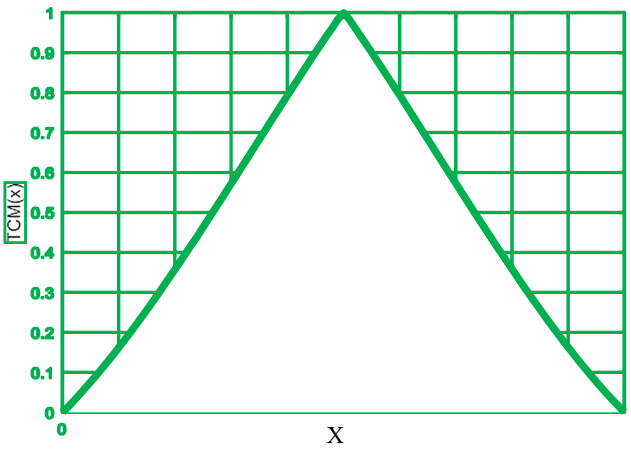


**Fig. 1** Iteration function of TCM for $\alpha = 1.42$

lessening and approaches back to zero once more. This shows that the iteration function has only one peak value. Therefore, TCM attains unimodality property at $\alpha = 1.42$. The bifurcation diagram is utilized for determining the next range of control parameter $\alpha$ in which the trigonometric chaotic map again attains unimodality property as shown in Fig. 1 for control parameter range $\alpha \in [1.3, 1.55]$.

The Schwarzian derivative is utilized for the analysis of the chaotic behavior of the trigonometric turbulent guide. The Schwarzian derivative, $S_{f(x)}$, of the trigonometric turbulent guide is shown in Eq. (2).

$$S_{f(x)} = \frac{f'''(x)}{f'(x)} - 1.5\left(\frac{f''(x)}{f'(x)}\right)^2 \tag{2}$$

As a whole, we can say that the trigonometric chaotic map fulfills the s-unimodality property at the specific starting values and control boundary. Another property to explore is the response against a little change in the starting values of the map. In Fig. 2, two sequences are shown which are

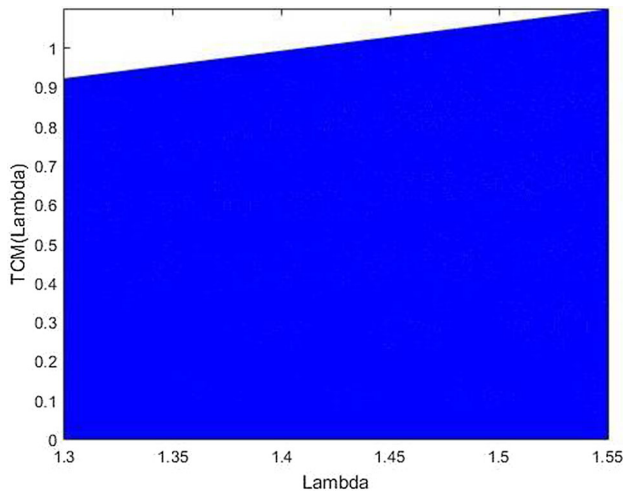


**Fig. 2** Bifurcation figure of TCM for $\alpha \in [1.3, 1.55]$

generated using TCM. The generated sequences become too much distinct after some iteration which shows the high sensitivity of TCM to a little change in starting values.

To explore the chaotic behavior of TCM, we have computed the Lyapunov exponent as represented by Eq. (3).

$$\alpha_{LE}(x_0) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln\left|f'(x_n, \alpha)\right| \tag{3}$$

In Fig. 3, the Lyapunov exponent that is created by the TCM is shown for parameter values ranging between [1, 1.6].

The experimental results obtained from the bifurcation diagram and the Lyapunov exponent indicate that the TCM exhibits chaotic behavior and also satisfies the s-unimodality property for $\alpha \in [1.3859, 1.4424]$. When a comparison of TCM is made with the logistic map and tent map for chaotic behavior and s-unimodality property, they also exhibit chaotic behavior and satisfy the s-unimodality property but for $\alpha \in [3.96, 4]$ and $\alpha \in [1.999, 2]$, respectively (Zhang et al. 2012). These values of $\alpha$ for the logistic map and tent map represent that TCM has a wide range of chaotic behavior making it secure for image encryption processes (Shabir et al. 2010).

To check whether TCM is suitable for an application in the field of cryptography, another important property that is "randomness" is investigated (Qin et al. 2018). For a keystream generator to be secured enough for application in the field of cryptography, it should not display deterministic properties. To experimentally verify whether the generated key streams by the TCM have random-like behavior or not, the NIST statistical suite is utilized (Yan and Bai 2017). The NIST suite is utilized to develop 15 statistical tests designed to test various sorts of irregularities in a binary sequence.

As a starting step, iterates generated by the TCM are first transformed into the binary sequence as shown in Eq. (4).

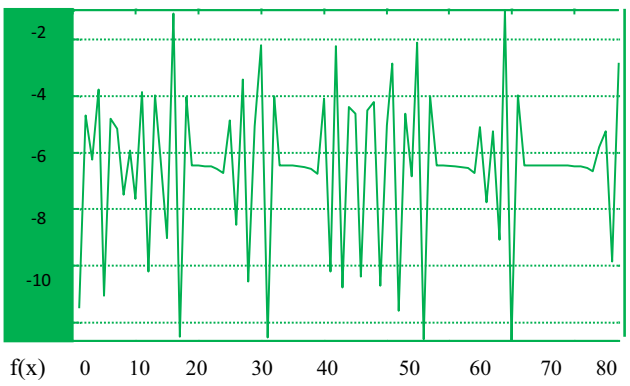


**Fig. 3** Schwarzian derivative of TCM for $\alpha = 1.42$

$$\beta_i = \begin{cases} 0 & 0 \le x_i < 0.5 \\ 1 & 0.5 \le x_i \le 1 \end{cases} \tag{4}$$

The degree of importance of "$\gamma$" for all NIST tests is fixed at 1%. This implies that out of 100 arrangements, one grouping is relied upon to be dismissed. For each statistical test, the $p$-esteem is additionally determined. In every test, if the degree of importance is not exactly the p-esteem, then the grouping is acknowledged as an arbitrary succession with a level of importance as close to 100%. If not, then the grouping is dismissed.

As Tables 1–3 show, the NIST statistical test suite is performed on a set of one hundred key streams of size 200,000 bits each created utilizing TCM, tent map, and logistic map, respectively. The $p$-values are calculated for each test, and the extent of key streams that fulfill the condition $\gamma \le p$-esteem is figured.

The TCM, as displayed in Table 1, has a better extent of key streams that pass the condition p-esteem $\ge 0.01$ than a tent and logistic maps. Besides, the $P$-upsides of $p$-values, determined with the assistance of the chi-square test, are on the whole higher than the degree of importance $\gamma$ if there should be an occurrence of the TCM and tent guide. However, the logistic map failed in three tests: block frequency, runs, and longest runs of ones (Figs. 4 and 5).

In the three guide results, the $p$-values are consistently circulated over the span (0, 1). For the TCM and tent map, since 0.01 is less than all $p$-values, so the generated key streams are considered random with a confidence level of 99%.

### 1.3 S-box using TCM

This has been proved that points generated by the TCM function are non-periodic, non-repeating, and can be used for encryption purposes (ref. TCM-paper). S-box can be created using the TCM Eq. (1) under Galois field (GF(2^n). A brief description of the Galois field is given in the following subsection.

### 1.4 Galois fields

Galois fields, often known as finite fields, are the foundations of any cryptographic theory, denoted by GF($p^n$), where p is any prime and $n \in Z^+$. If $n = 1$, then GF($p^n$) *is* known as the prime field. If $n > 1$, then GF($p^n$) is termed as the extension field. The order of the Galois fields is $p^n$. The Galois fields of order GF($p$) are simply the integers mod $p$, for $n > 1$, the elements of GF($p^n$) are polynomials of degree $n - 1$ with coefficients that take place from GF($p$).

**Table 1** S-box 1 using TCM over $GF(2^8)$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 71 | 224 | 96 | 164 | 146 | 129 | 185 | 233 | 124 | 155 | 52 | 235 | 101 | 249 | 134 | 3 |
| 186 | 102 | 138 | 94 | 4 | 97 | 77 | 121 | 176 | 92 | 5 | 175 | 158 | 214 | 241 | 201 |
| 152 | 128 | 74 | 169 | 30 | 99 | 179 | 187 | 45 | 148 | 60 | 123 | 90 | 120 | 180 | 117 |
| 150 | 42 | 110 | 225 | 147 | 65 | 50 | 252 | 245 | 162 | 183 | 182 | 58 | 145 | 106 | 253 |
| 170 | 131 | 139 | 12 | 103 | 14 | 236 | 205 | 105 | 9 | 8 | 154 | 125 | 10 | 33 | 255 |
| 1 | 114 | 237 | 137 | 95 | 35 | 87 | 209 | 84 | 223 | 130 | 229 | 89 | 113 | 63 | 231 |
| 167 | 62 | 86 | 195 | 78 | 26 | 196 | 251 | 204 | 188 | 194 | 242 | 184 | 67 | 177 | 143 |
| 157 | 222 | 208 | 34 | 136 | 193 | 141 | 119 | 49 | 220 | 59 | 100 | 247 | 115 | 116 | 212 |
| 142 | 192 | 57 | 111 | 248 | 104 | 202 | 17 | 161 | 68 | 159 | 238 | 165 | 200 | 230 | 181 |
| 93 | 75 | 51 | 21 | 69 | 55 | 47 | 254 | 2 | 199 | 190 | 174 | 168 | 25 | 178 | 126 |
| 61 | 160 | 38 | 171 | 22 | 151 | 32 | 132 | 83 | 172 | 156 | 149 | 133 | 153 | 109 | 127 |
| 122 | 76 | 44 | 64 | 166 | 37 | 23 | 218 | 228 | 15 | 70 | 191 | 163 | 215 | 226 | 211 |
| 0 | 216 | 108 | 72 | 54 | 56 | 36 | 40 | 27 | 24 | 28 | 135 | 18 | 41 | 20 | 227 |
| 221 | 85 | 31 | 207 | 43 | 203 | 239 | 6 | 39 | 189 | 13 | 7 | 98 | 118 | 243 | 232 |
| 173 | 144 | 112 | 80 | 48 | 19 | 82 | 219 | 73 | 11 | 206 | 197 | 210 | 16 | 250 | 66 |
| 244 | 88 | 81 | 46 | 213 | 140 | 91 | 217 | 29 | 79 | 198 | 107 | 53 | 246 | 240 | 234 |

**Table 2** S-box 2 using TCM over $GF(2^9)$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 48 | 90 | 154 | 124 | 153 | 22 | 84 | 104 | 97 | 138 | 130 | 63 | 116 | 77 | 27 |
| 71 | 44 | 108 | 161 | 196 | 162 | 109 | 152 | 188 | 23 | 93 | 9 | 123 | 182 | 151 | 117 |
| 95 | 49 | 132 | 191 | 1 | 131 | 144 | 110 | 64 | 149 | 129 | 200 | 70 | 190 | 26 | 137 |
| 45 | 100 | 50 | 139 | 87 | 201 | 10 | 179 | 232 | 237 | 242 | 229 | 210 | 207 | 145 | 62 |
| 105 | 140 | 195 | 33 | 51 | 210 | 165 | 11 | 211 | 98 | 233 | 24 | 122 | 228 | 163 | 118 |
| 32 | 175 | 202 | 185 | 166 | 52 | 171 | 85 | 12 | 168 | 65 | 206 | 218 | 7 | 69 | 150 |
| 81 | 133 | 220 | 225 | 0 | 76 | 43 | 111 | 103 | 251 | 244 | 193 | 96 | 115 | 173 | 28 |
| 46 | 31 | 72 | 221 | 125 | 53 | 178 | 243 | 212 | 13 | 197 | 239 | 219 | 25 | 199 | 60 |
| 94 | 174 | 30 | 155 | 236 | 249 | 250 | 205 | 170 | 252 | 5 | 245 | 66 | 114 | 183 | 121 |
| 3 | 159 | 203 | 34 | 247 | 254 | 253 | 54 | 215 | 238 | 80 | 241 | 209 | 189 | 146 | 61 |
| 106 | 99 | 230 | 222 | 231 | 9 | 19 | 246 | 213 | 169 | 14 | 234 | 180 | 59 | 29 | 91 |
| 89 | 184 | 20 | 167 | 126 | 186 | 177 | 39 | 127 | 55 | 79 | 15 | 255 | 227 | 136 | 119 |
| 134 | 176 | 147 | 235 | 248 | 4 | 88 | 226 | 38 | 112 | 56 | 83 | 217 | 67 | 158 | 6 |
| 141 | 160 | 194 | 74 | 240 | 35 | 143 | 18 | 37 | 214 | 148 | 208 | 17 | 198 | 40 | 78 |
| 21 | 107 | 223 | 156 | 204 | 224 | 172 | 187 | 181 | 216 | 157 | 57 | 192 | 164 | 135 | 120 |
| 82 | 101 | 73 | 142 | 47 | 75 | 36 | 86 | 102 | 42 | 128 | 113 | 58 | 92 | 68 | 41 |

#### 1.4.1 Addition and subtraction in GF($2^n$)

As we work on the field of characteristic 2, so the operation of addition and subtraction is the same. The addition of polynomials is very simple in the Galois field.

For example $(x^4 + x^2 + 1) + (x^5 + x^4 + 1) = x^5 + x^2$. This is just the usual addition in polynomials, but coefficients take place in $F_2$.

#### 1.4.2 Multiplication in GF($2^n$)

Let $f^*(x), g^*(x) \in \mathrm{GF}(2^n)[X]$,, and let $h^*(x)$ be the primitive polynomial whose degree is n. Then, their product denoted by $m^*(x)$ is given as$m^*(x) = (f^*(x) \cdot g^*(x)) \bmod h^*(x)$ and if $(f^*(x) \cdot a^*(x)) \bmod h^*(x) = 1$

Then, $a^*(x)$ is called the multiplicative inverse of $f^*(x)$.

Note that whenever we multiply two polynomials or find the multiplicative inverse of a polynomial, both require coefficient modulo 2 and the polynomials modulo $h(x)$.

## 2 Proposed S-box algorithm

In this section, we discuss two different S-box algorithm approaches. In the first technique, the nonlinear component of a block cipher is developed using trigonometric chaotic map interpreted over 256 order Galois field. In the second technique, instead of deploying 256-order Galois field-dependent S-boxes, we construct a different number of $8 \times 8$

**Table 3** S-box 3 using TCM over GF($2^{11}$)

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 48 | 90 | 154 | 124 | 153 | 22 | 84 | 104 | 97 | 138 | 130 | 63 | 116 | 77 | 27 |
| 71 | 44 | 108 | 161 | 196 | 162 | 109 | 152 | 188 | 23 | 93 | 9 | 123 | 182 | 151 | 117 |
| 95 | 49 | 132 | 191 | 1 | 131 | 144 | 110 | 64 | 149 | 129 | 200 | 70 | 190 | 26 | 137 |
| 45 | 100 | 50 | 139 | 87 | 201 | 10 | 179 | 232 | 237 | 242 | 229 | 210 | 207 | 145 | 62 |
| 105 | 140 | 195 | 33 | 51 | 210 | 165 | 11 | 211 | 98 | 233 | 24 | 122 | 228 | 163 | 118 |
| 32 | 175 | 202 | 185 | 166 | 52 | 171 | 85 | 12 | 168 | 65 | 206 | 218 | 7 | 69 | 150 |
| 81 | 133 | 220 | 225 | 0 | 76 | 43 | 111 | 103 | 251 | 244 | 193 | 96 | 115 | 173 | 28 |
| 46 | 31 | 72 | 221 | 125 | 53 | 178 | 243 | 212 | 13 | 197 | 239 | 219 | 25 | 199 | 60 |
| 94 | 174 | 30 | 155 | 236 | 249 | 250 | 205 | 170 | 252 | 5 | 245 | 66 | 114 | 183 | 121 |
| 3 | 159 | 203 | 34 | 247 | 254 | 253 | 54 | 215 | 238 | 80 | 241 | 209 | 189 | 146 | 61 |
| 106 | 99 | 230 | 222 | 231 | 9 | 19 | 246 | 213 | 169 | 14 | 234 | 180 | 59 | 29 | 91 |
| 89 | 184 | 20 | 167 | 126 | 186 | 177 | 39 | 127 | 55 | 79 | 15 | 255 | 227 | 136 | 119 |
| 134 | 176 | 147 | 235 | 248 | 4 | 88 | 226 | 38 | 112 | 56 | 83 | 217 | 67 | 158 | 6 |
| 141 | 160 | 194 | 74 | 240 | 35 | 143 | 18 | 37 | 214 | 148 | 208 | 17 | 198 | 40 | 78 |
| 21 | 107 | 223 | 156 | 204 | 224 | 172 | 187 | 181 | 216 | 157 | 57 | 192 | 164 | 135 | 120 |
| 82 | 101 | 73 | 142 | 47 | 75 | 36 | 86 | 102 | 42 | 128 | 113 | 58 | 92 | 68 | 41 |

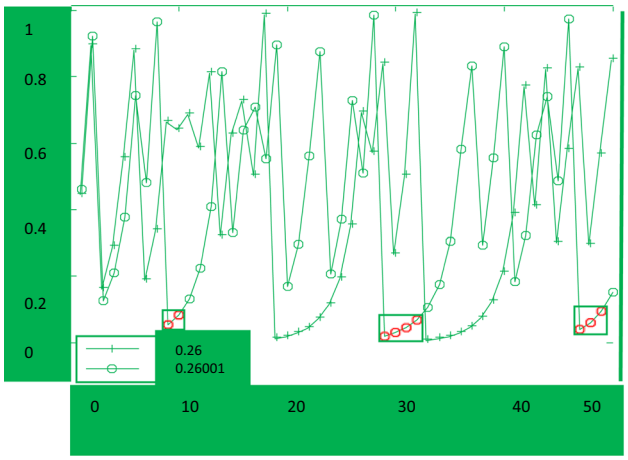


**Fig. 4** Two series acquired for ($x_0$, $\alpha$) = (0.26, 1.42), shown by squares, and for ($x_0$, $\alpha$) = (0.26001, 1.42), shown by circles

S-boxes using trigonometric chaotic map over GF($2^n$), for different odd values of $n \geq 9$.

## 2.1 Construction of S-box using trigonometric chaotic map over Galois field GF($2^8$)

Choose a primitive irreducible polynomial.

$$f(x) = x^8 + x^4 + x^3 + x^2 + 1 \tag{5}$$

One can choose independently any other primitive polynomial of degree 8 with coefficients in a binary field. Select trigonometric chaotic map. Choose $w_n = x_n$ and $w_{n+1} = y_n$

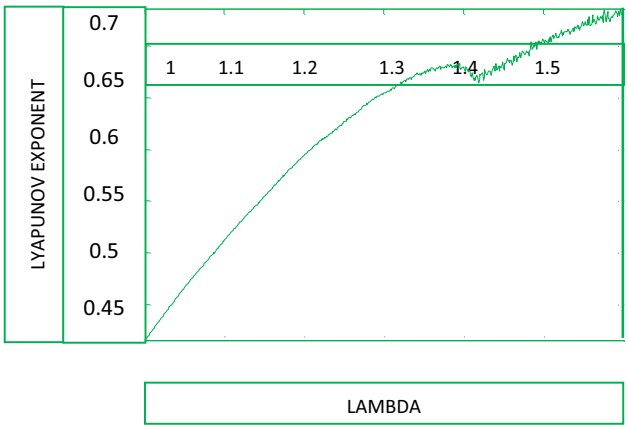


**Fig. 5** Lyapunov exponent of TCM for $\alpha \in [1, 1.6]$

$$w_{n+1} = \begin{cases} \alpha w_n \left[\sin\left\{\frac{\pi}{2} w_n\right\} + \cos\left\{\frac{\pi}{2} w_n\right\}\right] 0 \leq w_n \leq 0.5 \\ \alpha[1 - w_n]\left[\sin\left\{\frac{\pi}{2}(1 - w_n)\right\}\right. \\ \quad \left. + \cos\left\{\frac{\pi}{2}(1 - w_n)\right\}\right] 0.5 < w_n \leq 1 \end{cases} \tag{6}$$

where $w_{n+1} \in [0, 1]$, $w_0$ is the starting value and $\alpha$ is the control parameter. The purpose of selecting an irreducible polynomial is to construct the S-box over the Galois field (GF (2^8).

When we choose trigonometric chaotic map over GF($2^8$), the number of elements lying on it is $2^8 + 1$ including the point at infinity. The other thing we see is that whenever we choose this map over GF($2^8$), then there is no repetition in the $x$-coordinates, and repetition is accrued in $y$-values. The strength of this map is that it has 256 distinct

pairs of elements $(x, y)$ excluding the point at infinity over the GF($2^8$). Our requirement of generating an $8 \times 8$ S-box that has 256 distinct numbers is fulfilled by taking the $x$-coordinates of each ordered pair of points because there is no repetition in the $x$-coordinates elements and gives us exactly 256 elements. Apply inverse function under GF($2^8$) on each element of $x$-coordinate except zero elements with primitive irreducible polynomial given in Equation (5).

Finally, we have S-box having nonlinearity 112 which is given in Table 1. Figure 6 depicts the flowchart of the proposed algorithm.

## 2.2 Construction of S-box using trigonometric chaotic map over Galois field GF($2^n$)

The Galois fields GF($2^n$) of orders 512 and 1024 are utilized in this work to establish a more comprehensive and effective approach for the designing of a large number of distinct $8 \times 8$ S-boxes.

**Algorithm 1: Construction of S-box using TCM over $GF(2^8)$.**

1: **Input**: Choose a primitive irreducible polynomial of degree 8 with $b \in GF(2^8) - \{0\}$ and $S \leftarrow [0: 255]$.

2: **Output**: S-box

3: $A = \emptyset$

4: **for** each $x \in S$ **do**

5: **for** each $y \in S$ **do**

6: $\mathbf{w_n}$**=x** 7: $\mathbf{w_{n+1}}$**=y**

8: **if** $w_{n+1} = \begin{cases} \alpha w_n \left[\sin(\frac{\pi}{2} w_n) + \cos(\frac{\pi}{2} w_n)\right] & 0 \le w_n \le 0.5 \\ \alpha[1 - w_n][\sin\left(\frac{\pi}{2}(1 - w_n)\right) + \cos(\frac{\pi}{2}(1 - w_n))] & 0.5 < w_n \le 1 \end{cases}$ **then**

9: $x=w_n$

10: $y=w_{n+1}$

11: $A = A \cup \{x, y\}$.

12: **end if**

13: **end for**

14: **end for**

15: $B \leftarrow x$ coordinates from set $A$

16: $i \leftarrow 1: 256$

17: **if** $B(i) \leftarrow 0$ **then**

18: no change 19: **else** take inverse under $GF(2^8)$

20: **end if**

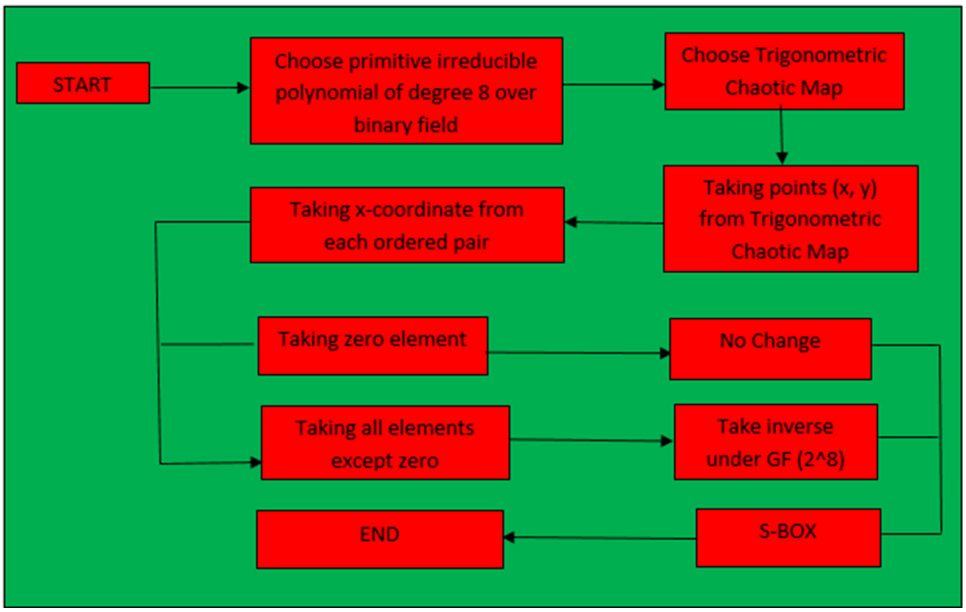


**Fig. 6** Flow chart of proposed S-box scheme based on TCM over GF (2^8)

#### 2.2.1 Construction of S-box using trigonometric chaotic map over Galois field GF($2^9$)

Firstly, choose a primitive polynomial.

$$f(x) = x^9 + x^4 + 1 \tag{7}$$

Over the binary field, any arbitrary primitive polynomial of degree 9 with coefficients in the binary field can be chosen independently. Choose a trigonometric chaotic map.

$$w_{n+1} = \begin{cases} \alpha w_n(\sin(\frac{\pi}{2}w_n) + \cos(\frac{\pi}{2}w_n))0 \le w_n \le 0.5 \\ \alpha(1-w_n)(\sin\left(\frac{\pi}{2}(1-w_n)\right) + \cos(\frac{\pi}{2}(1-w_n)))0.5 < w_n \le 1 \end{cases} \tag{8}$$

where $w_{n+1} \in [0, 1]$, $w_0$ is the starting value and $\alpha$ is the control parameter.

When we choose a trigonometric chaotic map over GF($2^9$), the number of elements lying on it is $2^9 + 1$ including the point at infinity. In this case, there is no repetition in the $x$-coordinates of points lying on it, and it gives us exactly $0 - 511$ elements and no repetition is accrued in the $y$-coordinates of map points and gives us random numbers. The specialty of this curve is that it has 512 distinct pairs of elements $(x, y)$ except the point at infinity over GF($2^9$). Take $y$-coordinate from each point lying on the map because of no repetition and randomness. Apply inverse function under GF($2^9$) on each element of $y$-coordinates except zero with primitive irreducible polynomial given in equation (7). As we required an $8 \times 8$ S-box which has 256 distinct numbers, take all elements randomly, which is less than 256. Finally, we get different S-boxes by giving different values to the parameter. As the number of primitive irreducible polynomials of degree 9 over GF(2) is 48, so through this technique, we can construct different $511 \times 48$ S-boxes. The S-box through this technique is presented in Table 2 having nonlinearity 106.25. The flow chart of the proposed technique is given in Fig. 7.

#### 2.2.2 Construction of S-box using trigonometric chaotic map over Galois field GF($2^{11}$)

Choose a primitive polynomial.

$$f(x) = x^{11} + x^4 + 1 \tag{9}$$

In the binary field, any arbitrary primitive irreducible of degree 11 with coefficients in the binary field can be elected independently. By selecting the trigonometric chaotic map given by:

$$w_{n+1} = \begin{cases} \alpha w_n[\sin(\frac{\pi}{2}w_n) + \cos(\frac{\pi}{2}w_n)]0 \le w_n \le 0.5 \\ \alpha[1-w_n][\sin\left(\frac{\pi}{2}(1-w_n)\right) + \cos(\frac{\pi}{2}(1-w_n))]0.5 < w_n \le 1 \end{cases} \tag{10}$$

where $w_{n+1} \in [0, 1]$, $w_0$ is the starting value and $\alpha$ is the control parameter.

The specialty of the map over GF($2^{11}$) is that the number of points $(x, y)$ lying on a map is $2^{11} + 1$ including the point at infinity. In this case, there is no repetition in $y$-coordinates of all points and random numbers, while in $x$-coordinates, there is no repetition but in the sequence. Skip the x-coordinates and take the y-coordinates of each pair of points to construct the robust S-boxes. Apply inverse function under GF($2^{11}$) on each $y$-coordinate except zero with primitive irreducible polynomial given in equation 9.

As we need 256 distinct numbers to construct an $8 \times 8$ S-box, choose randomly all elements which are less than 256. To construct a different number of S-boxes, one can vary the value of b. As the total number of primitive polynomials of degree 11 over the binary field is 176, one can construct the different number of $2047 \times 176$ S-boxes through this technique. The S-box through technique is given in Table 3, and a flow chart is presented in Fig. 7.

## 3 Proposed image encryption method

A summary of the steps of the proposed image encryption technique is shown below. The size of the original image is considered as M × N.

1. First of all, transform the size of the original image into 256 × 256 pixels.

**Algorithm 2: Construction of S-box using TCM over $GF(2^n)$**

1: **Input**: Choose primitive irreducible polynomial of degree n with $b \in GF(2^n) - \{0\}$ and $S \leftarrow [0: n-1]$

2: **Output**: S-box

3: $A = \emptyset$

4: **for** each $x \in S$ **do**

5: **for** each $y \in S$ **do**

6: $\mathbf{w_n = x}$ 7: $\mathbf{w_{n+1} = y}$

8: **if** $w_{n+1} = \begin{cases} \alpha w_n[\sin(\frac{\pi}{2}w_n) + \cos(\frac{\pi}{2}w_n)] & 0 \le w_n \le 0.5 \\ \alpha[1-w_n][\sin\left(\frac{\pi}{2}(1-w_n)\right) + \cos(\frac{\pi}{2}(1-w_n))] & 0.5 < w_n \le 1 \end{cases}$ **then**

9: $x = w_n$

10: $y = w_{n+1}$

11: $A = A \cup \{x, y\}$

12: **end if**

13: **end for**

14: **end for**

15: $B \leftarrow y$ coordinates from set $A$

16: $i \leftarrow 1: 2^n$

17: **if** $B(i) \leftarrow 0$ **then**

18: no change

19: **else** take inverse under $GF(2^n)$

20: **end if**

21: Take all random elements less than 256

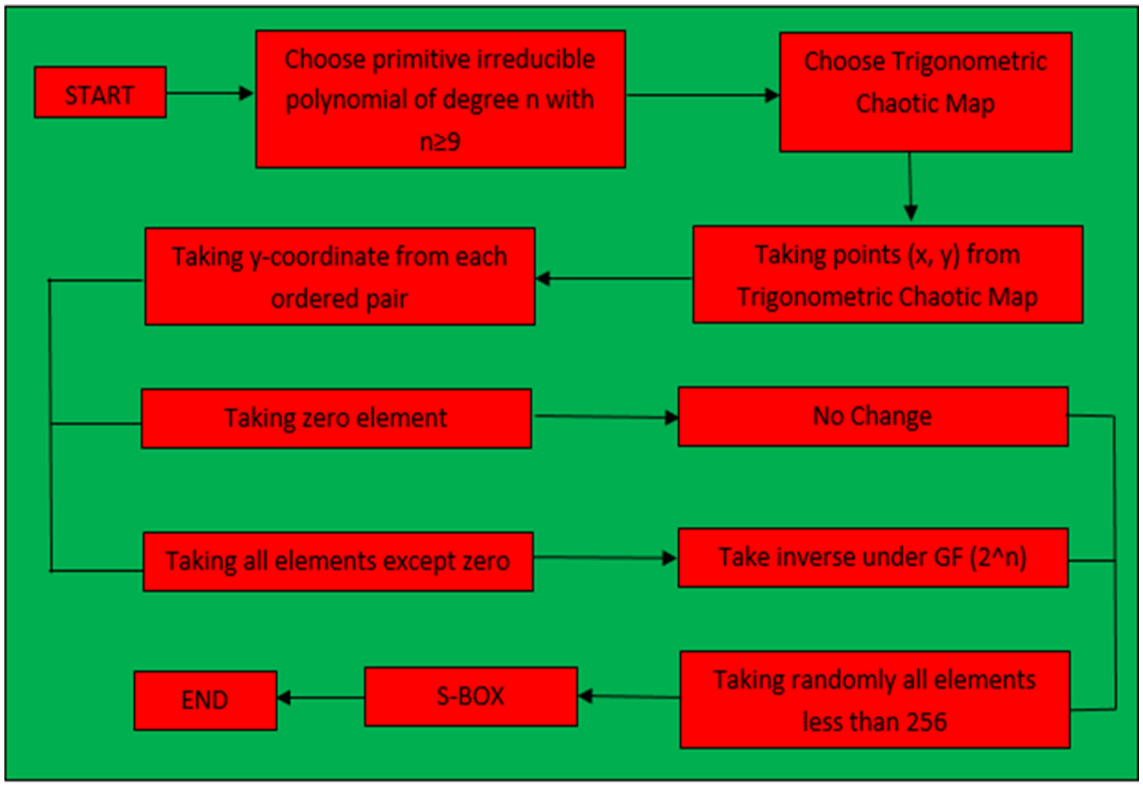


**Fig. 7** Flow chart of proposed S-box scheme based on TCM over GF($2^n$)

2. Next, consider a random image of the same size as an original image for confusion and diffusion processes.
3. After this, the original and random images are divided into square blocks where the size of each square is taken as m × m pixels.
4. "m" is worked out by utilizing the formula as shown in Eq. (11):

$$\mathrm{m} = \frac{\sqrt{M \times N}}{b^2} \tag{11}$$

In the above formula for finding "*m*," "*M*" represents the number of rows of the matrix corresponding to the image, "*N*" represents the number of columns of the matrix corresponding to the image, and "*b*" forms a portion of the secret key, along with the starting values and control parameter of TCM.In the above formula for finding "*m*," "*M*" represents

**Fig. 8** Lena image.jpg

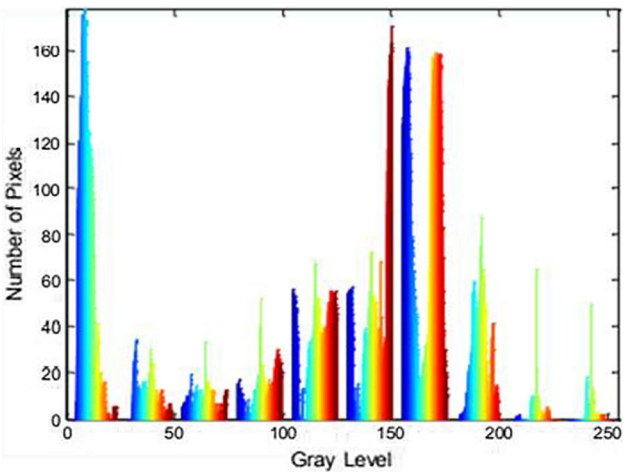


**Fig. 9** Histogram of Lena image

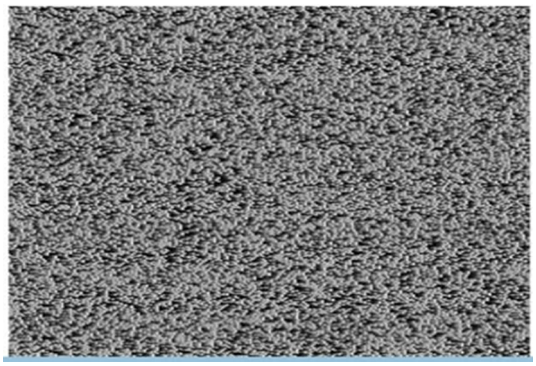

**Fig. 10** Encrypted image

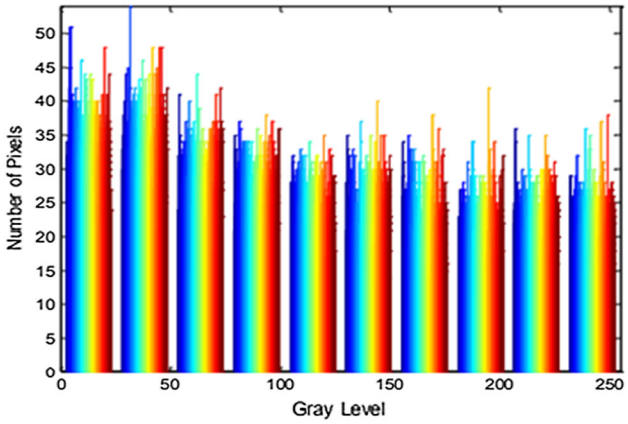


**Fig. 11** Histogram of Encrypted image

**Table 4** NIST statistical test suite results for 100 key streams of size 200,000-bit each generated by the TCM for control parameter $\alpha = 1.42$ and randomly chosen initial value

| Statistical test | *p*-value | Proportion |
|---|---|---|
| Frequency | 0.086568 | 0.93 |
| Block frequency | 0.303319 | 0.90 |
| Cumulative sums (forward) | 0.133368 | 0.91 |
| Cumulative sums (reverse) | 0.149881 | 0.92 |
| Runs | 0.987643 | 0.91 |
| Longest runs of one | 0.714019 | 0.92 |
| Rank | 0.782537 | 0.95 |
| Non-periodic-templates | 0.449021 | 0.99 |
| Overlapping-templates | 0.566655 | 0.92 |
| Approximate entropy | 0.291787 | 0.97 |
| Random-excursions($x = 1$) | 0.988728 | 0.98 |
| Random-excursions-variant ($x = 8$) | 0.673220 | 0.99 |
| Linear-complexity (substring length = 500) | 0.734538 | 0.92 |
| Serial 1 | 0.161917 | 0.98 |
| Serial 2 | 0.987119 | 0.96 |

**Table 5** NIST statistical test suite results for 100 key streams of size 200,000-bit each generated by the tent map for control parameter $\alpha = 1.9999$ and randomly chosen initial value

| Statistical test | *p*-value | Proportion |
|---|---|---|
| Frequency | 0.237282 | 0.95 |
| Block frequency | 0.158791 | 0.94 |
| Cumulative sums (forward) | 0.282249 | 0.93 |
| Cumulative sums (reverse) | 0.112325 | 0.96 |
| Runs | 0.393827 | 0.98 |
| Longest runs of one | 0.375450 | 0.96 |
| Rank | 0.893118 | 0.97 |
| Non-periodic-templates | 0.554637 | 0.95 |
| Overlapping-templates | 0.31404 | 0.96 |
| Approximate entropy | 0.213390 | 0.97 |
| Random-excursions($x = 1$) | 0.035118 | 0.98 |
| Random-excursions-variant ($x = 8$) | 0.739890 | 0.95 |
| Linear-complexity (substring length = 500) | 0.825326 | 0.99 |
| Serial 1 | 0.564146 | 0.99 |
| Serial 2 | 0.235387 | 0.96 |

the number of rows of the matrix corresponding to the image, "$N$" represents the number of columns of the matrix corresponding to the image, and "$b$" forms a portion of the secret key, along with the starting values and control parameter of TCM.

5. The following steps are performed on each square block of original and random images.
   a. The corresponding square of original and random images is changed over into a row vector. Perform XOR on the row vector of the original image and random image to obtain a row vector.
   b. A row vector, of size [1, m × m], is obtained by using TCM to create pseudorandom numbers. The produced numbers are utilized as pixel location files to rearrange pixel areas of the row vector.
   c. Pixel intensity estimation of the scrambled row vector, obtained from the previous step, is changed according to Eq. (12).

$$K = \mathrm{Sin}\,(K + b) + K \tag{12}$$

   where $K$ is a created key stream utilizing TCM and b is the acquired line vector having performed XOR of original and random row vectors from the past advance.
   d. The resultant row vector is changed over into a square, of size m × m pixels and secured to shape the encoded image. Finally, encryption is made using XOR with S-box and image matrices

**Table 6** NIST statistical test suite results for 100 key streams of size 200,000-bit each generated by the logistic map for control parameter $\alpha = 1.9999$ and randomly chosen initial value

| Statistical test | *p*-value | Proportion |
|---|---|---|
| Frequency | 0.519021 | 0.99 |
| Block frequency | 0.103201 | 0.93 |
| Cumulative sums (forward) | 0.811413 | 0.98 |
| Cumulative sums (reverse) | 0.295709 | 0.99 |
| Runs | 0.00001 | 0.78 |
| Longest runs of one | 0.000950 | 0.96 |
| Rank | 0.967835 | 0.97 |
| Non-periodic-templates | 0.898139 | 0.99 |
| Overlapping-templates | 0.395326 | 0.97 |
| Approximate entropy | 0.026989 | 0.98 |
| Random-excursions($x = 1$) | 0.544631 | 0.99 |
| Random-excursions-variant ($x = 8$) | 0.213991 | 0.99 |
| Linear-complexity (substring length = 500) | 0.494729 | 0.97 |
| Serial 1 | 0.755679 | 0.99 |
| Serial 2 | 0.513763 | 0.98 |

6. Pixel's intensity estimations of the encoded image are changed utilizing (12).

## 4 Experimental results

The achievement of the suggested image encryption method is checked using the well-known image of Lena. The proposed encryption method is implemented using MATLAB and Intel core I3 with a 4 GB memory machine. The Lena image is used for testing purposes as displayed in Fig. 8. The non-uniform histogram of the Lena picture is displayed in Fig. 9. The parameter "b" in Eq. (12) to find "m" (the block size) is set to four which results in a $16 \times 16$ block. Figure 9 shows the encrypted image of Lena which is obtained after the implementation of the proposed image encryption method. The histogram of the encrypted image is displayed in Fig. 10. The histogram in Fig. 10 shows the semi-uniform distribution of encrypted image pixels. This indicates the robustness of the encryption method against histogram attack methods. Encryption immunity against Brute force attack methods is also investigated. According to the literature, for an encryption algorithm to be safe enough against Brute force attack methods it should have a complexity of the order O ($2^{128}$). Trial results show that the suggested encryption technique has a complexity of order O ($2^{169}$). Encryption immunity against the high correlation between adjacent image pixels is investigated. For this reason, horizontal, vertical, and corner relationships between any of the two next to each other pixels are figured by utilizing Eq. 13.

$$r = \frac{2\sum_{i=1}^{2}(x_i,\ y_j) - \sum_{i=1}^{2}(x_i)\sum_{i=1}^{2} y_i}{\sqrt{\left(2\sum_{i=1}^{2} x_i^2 - \sum_{i=1}^{2} x_i\right)^2)(2\sum_{i=1}^{2} y_i^2 \sum_{i=1}^{2} y_i)^2}} \tag{13}$$

where "$r$" represents the "correlation coefficient." To calculate horizontal, vertical, and diagonal correlation one thousand side-by-side pixels are randomly selected. The encryption performance of the proposed trigonometric chaotic map is compared with the performances of well-

**Table 7** Correlation results of one thousand neighboring pixels randomly selected from original and encrypted images

| | Original image | TCM-based encrypted image $\alpha = 1.39$ | NCA-based encrypted image $\alpha = 3.5$ | LM-based encrypted image $\alpha = 3.97$ |
|---|---|---|---|---|
| Horizontal correlation | 0.9406 | 0.0231 | 0.1737 | 0.2034 |
| Vertical correlation | 0.9764 | 0.0509 | 0.0471 | 0.203 |
| Diagonal correlation | 0.9133 | 0.0382 | 0.0553 | 0.0275 |
| Average correlation | 0.9320 | 0.0305 | 0.0720 | 0.0876 |

**Table 8** Entropy of Encrypted Image

| | Original image | TCM-Based encrypted image $\alpha = 1.39$ | TCM + S-BOX based encrypted image $\alpha = 1.39$ | LM-Based encrypted image $\alpha = 3.97$ |
|---|---|---|---|---|
| Entropy | 7.0097 | 7.8992 | 7.9448 | 7.7496 |

known chaotic maps such as logistic maps, and nonlinear chaotic maps (Eqs. 14, and 15) as displayed in Table 4.

The experimental results obtained from the bifurcation diagram and the Lyapunov exponent indicate that the TCM exhibits chaotic behavior and also satisfies the s-unimodality property for $\alpha \in [1.3859, 1.4424]$. When a comparison of TCM is made with the logistic map and tent map for chaotic behavior and s-unimodality property, they also exhibit chaotic behavior and satisfy the s-unimodality property but for $\alpha \in [3.96, 4]$ and $\alpha \in [1.999, 2]$, respectively. These values of $\alpha$ for the logistic map and tent map represent that TCM has a wide range of chaotic behavior making it secure for image encryption processes (Fig. 11).

According to the results mentioned in Table 4, the correlation between pixels of the original image is very high. Results also indicate that the relationship between pixels of the scrambled picture is exceptionally low. On comparing an average correlation value of the proposed trigonometric chaotic map with other maps, it acquires the best average results. Also, entropy is utilized for calculating the quantity of randomness in an image. According to the results mentioned in Table 4, the entropy value of the original image is very low. In contrast, the entropy values obtained from the scrambled picture are high. An ideal value of entropy is 8. The encryption method based on the Tent map accomplishes the best entropy results. But, the TCM also acquires entropy results close to TM-based encryption method. Since the entropy value of the proposed image encryption method is close to the ideal value, i.e., 8, this shows the robustness of the proposed method in opposition to entropy attack methods. As a whole, the acquired semi-uniform histogram, statistical correlation, and entropy values show the higher level of permutation and replacement properties of the proposed method (Tables 5, 6, 7 and 8).

$$x_{n+1} = \alpha x_n(1 - x_n) \tag{14}$$

$$x_{n+1} = \left(1 - \alpha^{-4}\right)\cot\left(\frac{\alpha}{1+\alpha}\right)\left(1 + \frac{1}{\alpha}\right)^{\alpha}\tan(\gamma x_n)(1 - x_n)^{\alpha} \tag{15}$$

## 5 Conclusion

In this research, we developed a more secure and fastest image cryptosystem dependent on a trigonometric chaotic map and double XOR of an arbitrary image with S-boxes (developed by a trigonometric chaotic map). To make the encryption more secure and unbreakable, we utilized a basic chaotic map, produced a row vector of the original and a random image. The confusion and diffusion are obtained in a row-wise approach like Exclusive-OR produced a row vector that further applied a TCM resulting in the form of the encrypted image which was further encrypted by taking XOR with S-boxes. Usual tests are performed for the security of the algorithm; results are produced and presented.

**Author's contribution** The proposed method enhances the security of messages (images) transmitted via the internet. Which is beneficial for Banking sector, security agencies, society and the individuals working in the field of cybersystem/cryptography/network security.

**Funding** The authors have not disclosed any funding.

**Data availability** Enquiries about data availability should be directed to the authors.

## Declarations

**Competing Interests** The authors have not disclosed any competing interests.

## References

Abd-El-Hafiz SK, Radwan AG, AbdEl-Haleem SH (2015) Encryption applications of a generalized chaotic map. Appl Mathemat Inform Sci 9(6):3215–3233

Abu-Amara F (2018) Image encryption using trigonometric chaotic map. J Adv Res Dyn Control Syst 10(13):230–237

Abu-Amara F, Abdel-Qader I (2013) Chaotic image encryption via convex sinusoidal map. WSEAS Trans Signal Process 9(4):177–184

Agarwal S (2018) Secure image transmission using fractal and 2D-chaotic map. J Imaging 4(1):17

Bano M, Shah TM, Shah T (2016a) Genetic algorithm on piecewise linear chaotic map bases image encryption. Indian J Sci Technol 9(8):1–7

Bano M, Shah T, Talat R, Shah TM (2016b) Image reconstruction and text embedding using graph cut. Sci Int 28(2):905–911

Bano M, Shah T, Talat R, Shah TM (2017) Image reconstruction and text embedding using scan patterns with XOR in graph cut technique. J Intell Fuzzy Syst 33(2):1097–1104

Bano M, Abdullah S, Shah TM, Panityakul T, Chinram R (2020) An extended image encryption with Markov processes in solutions images dynamical system of non-linear differential equations. J Mathemat Comput Sci 10(6):2191–2207

Duan X, Liu J, Zhang E (2019) Efficient image encryption and compression based on a VAE generative model. J Real-Time Image Proc 16:765–773

Guanghui C, Kai H, Yizhi Z, Jun Z, Xing Z (2014) Chaotic image encryption based on running-key related to plaintext. Sci World J 490179:1–9

Jin H, Ashraf S, Abdullah S, Qiyas M, Bano M, Zeng S (2019) Linguistic spherical fuzzy aggregation operators and their applications in multi-attribute decision making problems. Mathematics 7(5):413. https://doi.org/10.3390/math7050413

Khan AA, Qiyas M, Abdullah S, Luo J, Bano M (2019) Analysis of robot selection based on 2-tuple picture fuzzy linguistic aggregation operators. Mathematics 7(10):1000. https://doi.org/10.3390/math7101000

Lawnik M (2017) Generalized logistic map and its application in chaos based cryptography. J Phys: Conf Ser 936(1):012017

Liu L, Miao S (2017) An image encryption algorithm based on Baker map with varying parameter. Multimed Tools Appl 76:16511–16527

Liu L, Hao S, Lin J, Wang Z, Hu X, Miao S (2018) Image block encryption algorithm based on chaotic maps. IET Signal Proc 12(1):22–30

Paar C (2014) Understanding cryptography: a textbook for students and practitioners. Springer, New York

Panityakul T, Bano M, Shah TM, Prangchumpol D (2022) An RGB color image double encryption scheme. Int J Math Comput Sci 17(1):183–194

Qin C, Zhou Q, Cao F, Dong J, Zhang X (2018) Flexible lossy compression for selective encrypted image with image inpainting. IEEE Trans Circuits Syst Video Technol 29(11):3341–3355

Shabir M, Jun YB, Bano M (2010) On prime fuzzy bi-ideals of semigroups. Iran J Fuzzy Syst 7(3):115–128

Sheela S J, Suresh K V, & Tandur D (2017) Secured text communication using chaotic maps. In: 2017 international conference on algorithms, methodology, models and applications in emerging technologies 1–6

Sui L, Duan K, Liang J, Hei X (2014) Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. Opt Express 22(9):10605–10621

Thinnukool O, Panityakul T, Bano M (2021) Double encryption using trigonometric chaotic map and XOR of an image. Comput Mater Continua. https://doi.org/10.32604/cmc.2021.019153

Yan B, & Bai S (2017) Design of image confusion-diffusion cryptosystem based on vector quantization and cross the chaotic map. In: 2017 2nd international conference on image, vision, and computing 639–644

Zhang X, Feng G, Ren Y, Qian Z (2012) Scalable coding of encrypted images. IEEE Trans Image Process 21(6):3108–3114