Highly Secured and Quickest Image Encryption Algorithm Based on Trigonometric Chaotic Map and S-Box

Ronnason Chinram
Prince of Songkla University - Hat Yai Campus: Prince of Songkla University
Mahwish Bano
Air University
Umair Habib
Air University
Pattarawan Singavananda (pattarawan.pe@skru.ac.th)
Songkhla Rajabhat University https://orcid.org/0000-0002-0261-6816

Research Article

Keywords: Encryption, Image Encryption, S-Box, Trigonometric Chaotic Map, XOR

Posted Date: June 21st, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1532329/v1

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], *

[1] Division of Computational Science, Faculty of Science, Prince of Songkla University, Hat Yai, Songkhla 90110, Thailand, Email: ronnason.c@psu.ac.th

[2]Department of Mathematics, Air University, Islamabad, 44000, Pakistan, Email: mahwish@mail.au.edu.pk, 191764@students.au.edu.pk

[3]Bachelor of Science (Mathematics), Faculty of Science and Technology, Songkhla Rajabhat University, Songkhla 90000, Thailand, Thailand, Email: pattarawan.pe@skru.ac.th

* Corresponding author

E-mail: pattarawan.pe@skru.ac.th

Abstract:

A significant number of image encryption plans have been proposed during the latest years. By far most of 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. Propelled by this, we propose another proficient and quick image encryption plan subject to the Trigonometric turbulent aide. In contrast to the most of 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 of adjoining pixels and non-repeating sequences. By then, we join the XOR activity with modulo capacity to cover the pixel esteems and thwart 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). Finally, encryption is made using XOR with S-box and image matrices. High security is achieved due to non-repeating sequence of trigonometric chaotic map. Reversal is quick and flawless.

Keywords: Encryption; Image Encryption; S-Box; Trigonometric Chaotic Map; XOR

1 INTRODUCTION:

The speedy improvement of interactive media innovation and PC networks notwithstanding the expanded use of cloud-based capacity and huge information require techniques to ensure individuals' private and secret information [4-12]. Simultaneously, the pre-owned insurance strategy ought to be exceptionally secure without compromising the usefulness and ease of use of

the framework to give comfort to clients [1]. Picture encryption is one of the ordinarily utilized and compelling techniques to ensure pictures during capacity and transmission [13]. 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 [14]. Turbulent guides hold alluring qualities, for example, unsteadiness of framework circle, basic execution, high affectability to a little change in starting condition and control boundaries, and pseudorandom [15]. Distinctive turbulent guides were accounted for in the writing like convex sinusoidal map, parameter-varying baker map [16], cross a chaotic map, generalized sine map, combined sine and tent map, generalized logistic map, and a few others. Each proposed turbulent guide enjoys its benefits and hindrances as far as encryption time, security, and intricacy [2].

The strategic guide, quite possibly the most normally utilized tumultuous guides, 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 [3]. It was tracked down that the vast majority of the turbulent cryptosystems have deficient heartiness and security. Another work detailed that the logistic guide, Mandelbrot map, and symmetric tent guide hold a huge arrangement of weaknesses [17].

A one-dimensional turbulent guide is proposed in this paper; the trigonometric chaotic map (TCM). Then, at that point, the qualities of the TCM are researched. The examined qualities are affectability to a little change in starting condition, tumultuous conduct, s-unimodality, and haphazardness. In light of the examined qualities, a picture encryption strategy is created. At last, measurable properties and encryption execution of the created picture encryption strategy are broken down.

1.1 Trigonometric Chaotic Map:

Equation (1) shows the proposed trigonometric chaotic map.

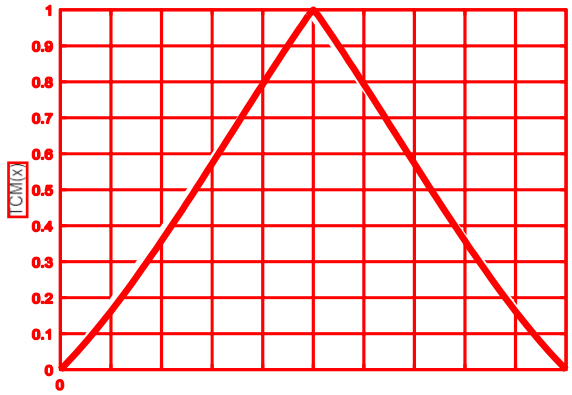
$$w_{n+1} = \begin{cases} \alpha w_n \left[sin\left\{\frac{\pi}{2} w_n\right\} + cos\left\{\frac{\pi}{2} w_n\right\}\right] & 0 \le w_n \le 0.5 \\ \alpha[1 - w_n]\left[sin\left\{\frac{\pi}{2}(1 - w_n)\right\} + cos\left\{\frac{\pi}{2}(1 - w_n)\right\}\right] & 0.5 < w_n \le 1 \end{cases} \quad (1)$$

Where $w_{n+1} \in [0, 1]$, w_0 is the starting value and α is the control boundary.

1.2 Analysis of TCM Properties:

In this part, 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. The below 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 continues to increment till it achieves the pinnacle worth of 1

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



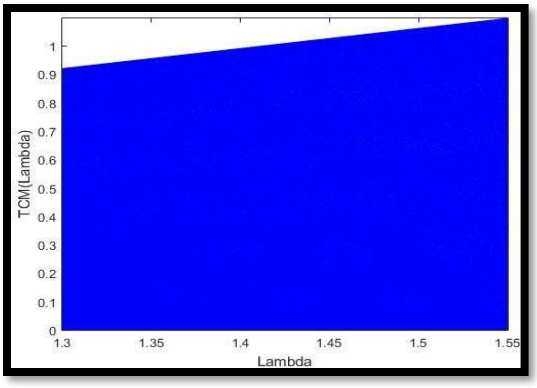


Figure 1: Iteration function of TCM for α = 1.42 **Figure 2: The bifurcation figure of TCM for α ∈ [1.3, 1.55]**

The Schwarzian derivative is utilized for the analysis of the chaotic behavior of the trigonometric turbulent guide. The Schwarzian derivative of the trigonometric turbulent guide is shown in Equation (2).

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

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 figure (2) two sequences are shown which are 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.

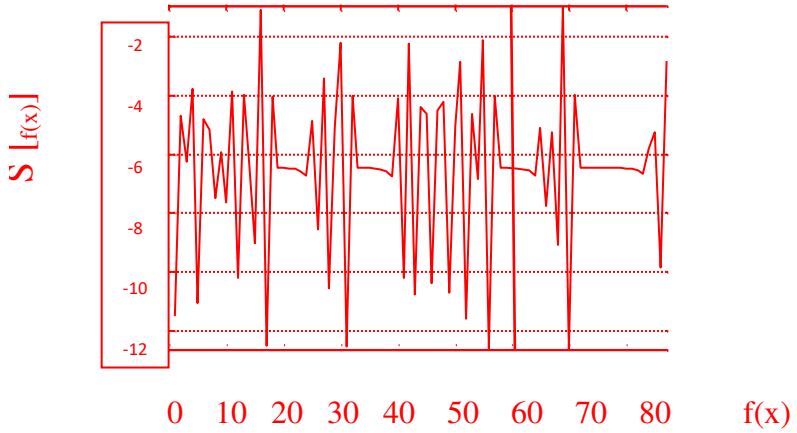


Figure 3: The schwarzian derivative of TCM for α = 1.42.

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

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

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

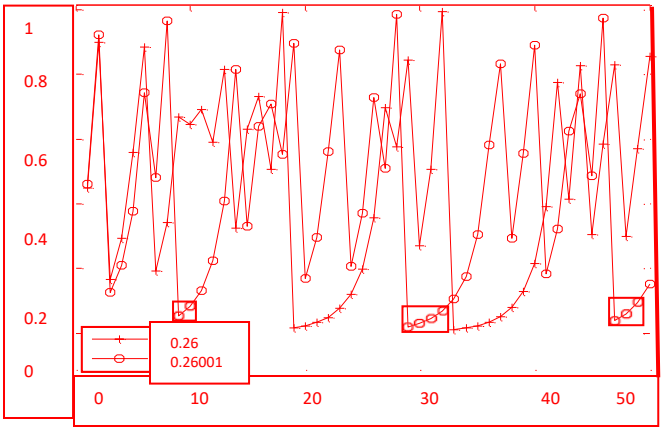


Figure 4: Two series acquired for (x_0, α) = (0.26, 1.42), shown by squares, and for (x_0, α) = (0.26001, 1.42), shown by circles.

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 α ∈ [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 α ∈ [3.96, 4] and α ∈ [1.999, 2] respectively. These values of α for logistic map and tent map represent that TCM has a wide range of chaotic behavior making it secure for image encryption processes.

To check whether TCM is suitable for applying in the field of cryptography, another important property that is "randomness" is investigated. For a key-stream generator to be secure enough for application in the field of cryptography, it should not display deterministic properties. To experimentally verify that whether the generated key-streams by the TCM have random-like behavior or not the NIST statistical suite is utilized [1]. 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 firstly transformed into the binary sequence as displayed in Equation (4).

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

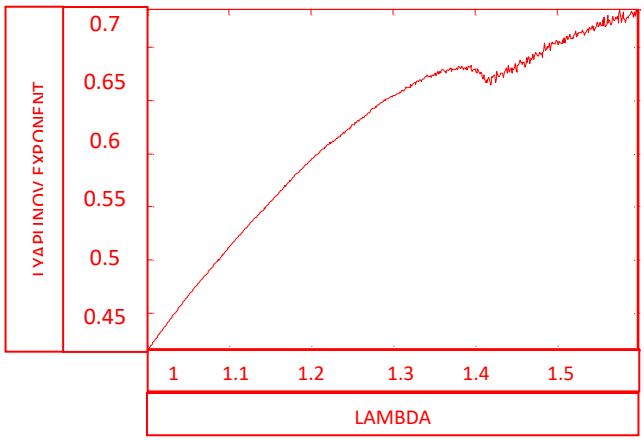


Figure 5: The Lyapunov exponent of TCM for α ∈ [1, 1.6].

The degree of importance of "γ" for all NIST tests is fixed to 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 200000 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 γ ≤ p-esteem is figured.

The TCM, as displayed in Table 1, has a better extent of key-streams that pass the condition p-esteem ≥ 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 γ 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.

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%.

1.4 Creation of S-box using TCM:

This has been proven 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 function (1) under Galois Field (GF(2^n)). A brief description of the Galois field is given in the following subsection.

1.4.1 *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 $GF(p)$.

1.4.2 *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 usual addition in polynomials, but coefficients take place in F_2.

1.4.3 *Multiplication in* $GF(2^n)$:

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

$$m^*(x) = \left(f^*(x) \cdot g^*(x)\right) \ mod\ h^*(x) \quad \text{And if} \quad \left(f^*(x) \cdot a^*(x)\right) \ mod\ h^*(x) = 1$$

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

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

2 Proposed S-box Algorithm:

In this section, we discussed 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 8×8 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 primitive polynomial. $f(x) = x^8 + x^4 + x^3 + x^2 + 1$ (5)

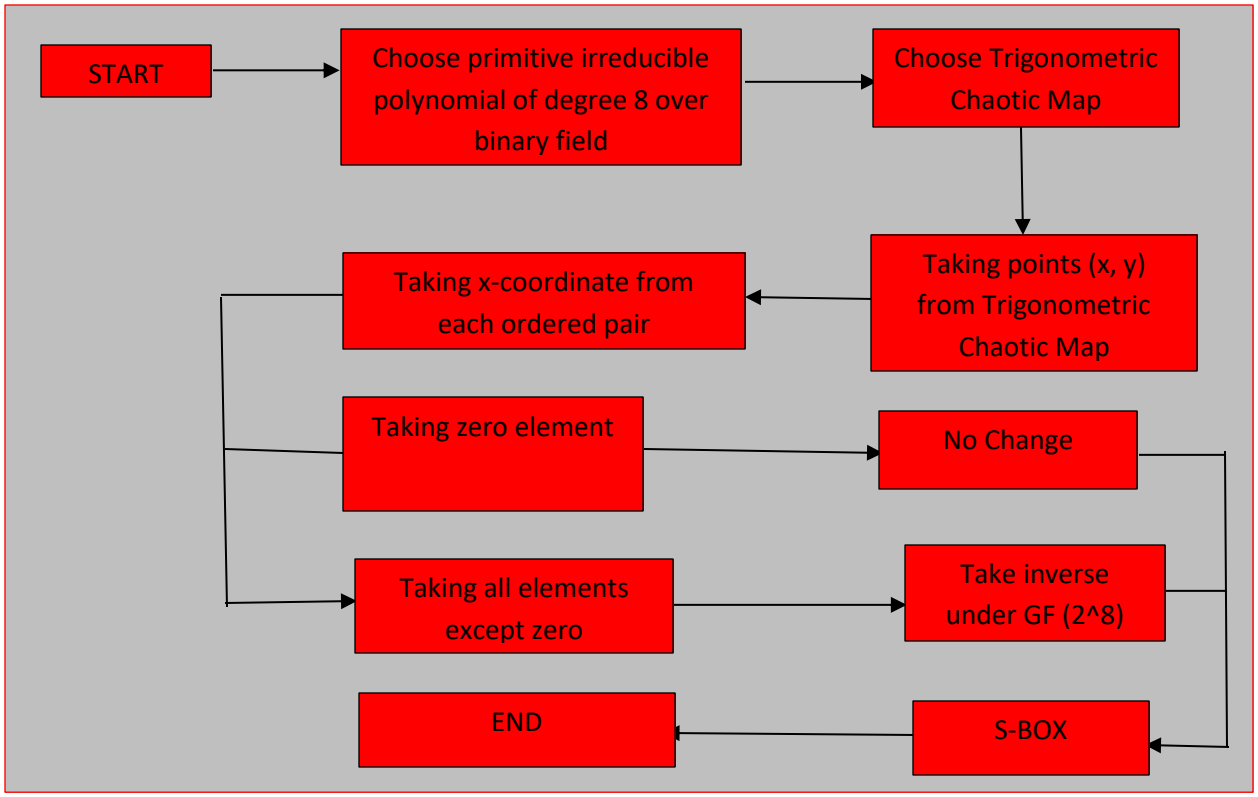
One can choose independently any other primitive polynomial of degree 8 with coefficients in a binary field. Selecting Trigonometric chaotic map. Choose $w_n = x_n$ and $w_{n+1} = y_n$

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

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 8×8 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.

Figure 6: Proposed S-box scheme based on TCM over GF (2^8)



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

1: **Input**: Choose 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**

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

2.2 *Construction of S-box using Trigonometric Chaotic Map over Galois field* $GF(2^n)$:

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

2.2.1 *Construction of S-box using Trigonometric Chaotic Map over Galois field* $GF(2^9)$

Firstly, choose a primitive polynomial. $f(x) = x^9 + x^4 + 1$ (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.

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

When we choose 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 x-coordinates of points lying on it and 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 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 (8). As we required 8×8 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 511×48 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 figure 7.

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

Choose primitive polynomial.

$f(x) = x^{11} + x^4 + 1$ (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:

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

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 y-coordinates of each pair of points to construct the robust S-boxes. Apply inverse function under $GF(2^{11})$ on each y-coordinates except zero with primitive irreducible polynomial given in equation (9). As we need 256 distinct numbers to construct an 8×8 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 binary field is 176, one can construct the different number of 2047×176 S-boxes through this technique. S-box through technique is given in table 3, and a flow chart is presented in figure 7.

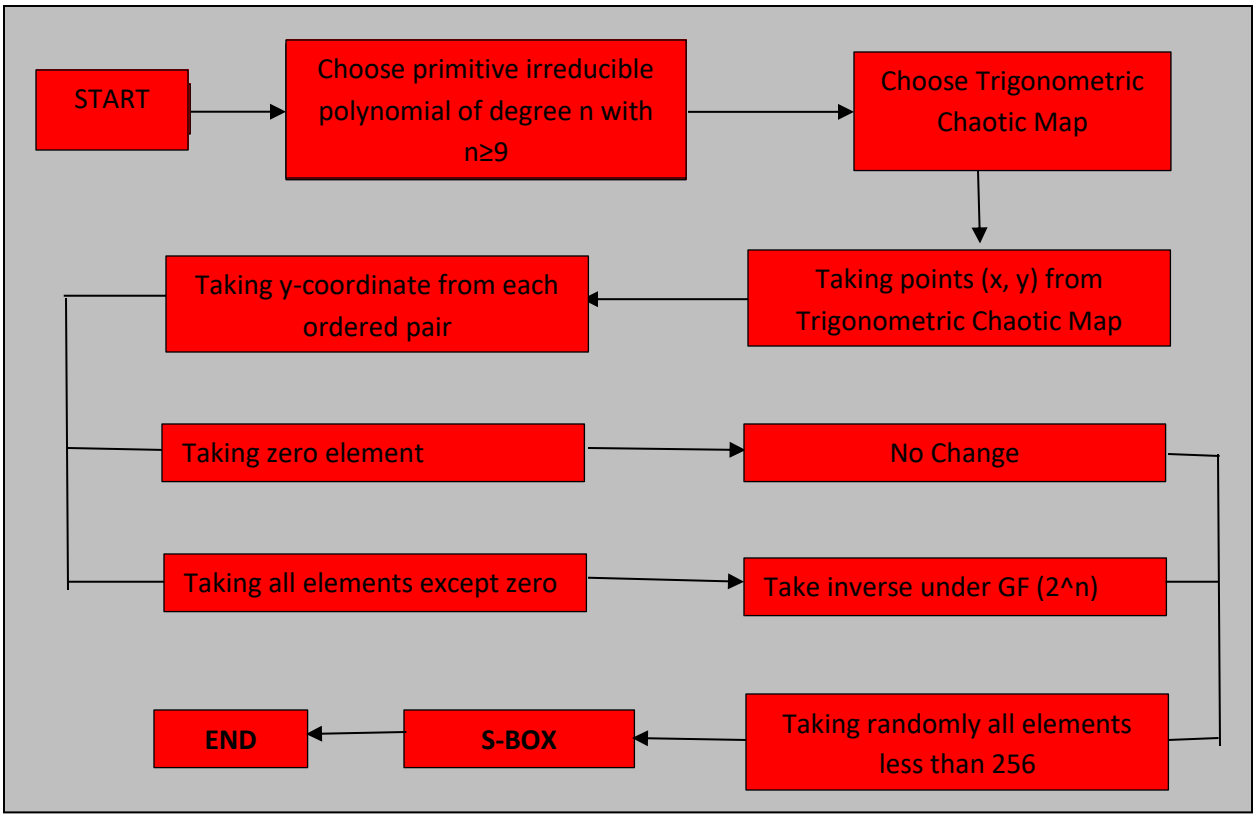


Figure 7: Proposed S-box scheme based on TCM over $GF(2^n)$

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

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

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

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.
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 Equation (11):

$$m = \frac{\sqrt{M \times N}}{b^2} \quad (11)$$

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.

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 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 Equation (12).
    $$K = \text{Sin}(K + b) + K \quad (12)$$
    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
6. Pixel's intensity estimations of the encoded image are changed utilizing (12).

Figure 8: Lena image.jpg

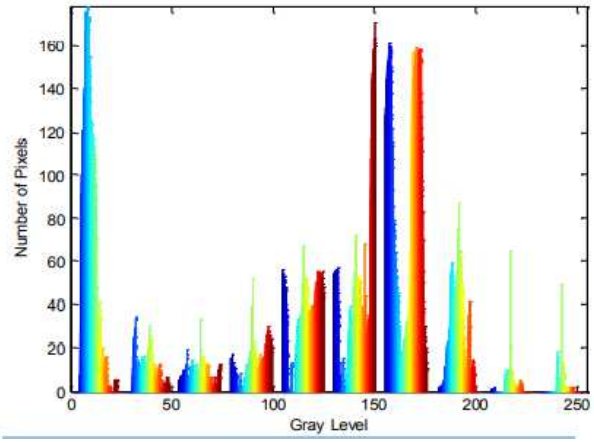


Figure 9: Histogram of Lena image.

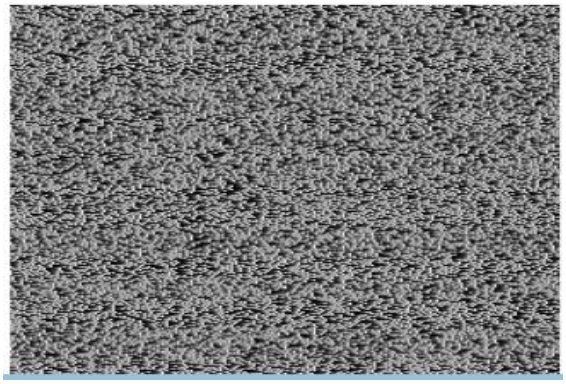


Figure 10: Encrypted image.

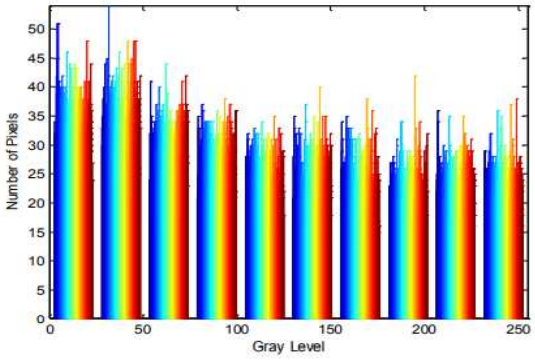


Figure 11: Histogram of the encrypted image.

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 4GB memory machine. The Lena image is used for testing purposes as displayed in Figure (8). The non-uniform histogram of the Lena picture is displayed in figure (9). The parameter "b" in equation (12) to find "m" (the block size) is set to four which results in a 16 × 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 Figure (10). The histogram in Figure (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 an intricacy 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 the below-mentioned Equation 13.

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

Where "r" represents "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-known chaotic maps such as logistic map, non-linear chaotic map, and tent map (Equations 8, 9, 10) as displayed in table 4.

According to the results as 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 as 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.

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

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

$$x_{n+1} = \begin{cases} \alpha x_n \ , & x_n < 0.5 \\ \alpha(1 - x_n) \ , & x_n \geq 0.5 \end{cases} \tag{16}$$

Table 1: NIST statistical test suite results for 100 key streams of size 200000-bit each generated by the TCM for control parameter α =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 ones	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 2: NIST statistical test suite results for 100 key streams of size 200000-bit each generated by the tent map for control parameter α =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 ones	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

Table 3: NIST statistical test suite results for 100 key-streams of size 200000-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 ones	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

Table 4: Correlation results of one thousand neighboring pixels randomly selected from original and encrypted images.

	Original image	**TCM-Based encrypted image α = 1.39**	**NCA-Based encrypted image α = 3.5**	**LM-Based encrypted image α = 3.97**	**TM-Based encrypted image α = 1.9999**
Entropy	7.0097	7.8992	7.0707	7.7496	7.988
Horizontal Correlation	0.9406	0.0231	0.1737	0.2034	0.0436
Vertical correlation	0.9764	0.0509	0.0471	0.203	0.13096
Diagonal correlation	0.9133	0.0382	0.0553	0.0275	0.0361
Average correlation	0.9320	0.0305	0.0720	0.0876	0.05

5 Conclusion:

In this paper, 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 trigonometric chaotic map). To make the encryption more secure and unbreakable, we utilized a basic chaotic map; produced a row vector of original and a random image. The confusion and diffusion are obtained in a row-wise approach like XOR produced a row vector which further applied a TCM resulted in the form of the encrypted image which further encrypted by taking XOR with S-boxes. Usual tests are performed for the security of the algorithm, results are produced and presented.

Authors contribution

The authors contributed to each part of this paper equally.

Funding

No funding was received.

Declarations

Conflict of interest

The authors declare that they have no conflict of interest.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent

Informed consent was obtained from all individual participants included in the study.

References:

[1] Dhingra, S., Savalgi, A.A., & Jain, S. Laplace Transformation based cryptographic technique in network security. **International Journal of Computer Applications, 136(7), 0975-8887.** doi: 10.5120/ijca2016908482.

[2] Elzaki, T.M. (2011). The new integral transform Elzaki transform. **Global Journal of Pure and Applied Mathematics, 7(1), 57-64.**

[3] Hiwarekar, A.P (2012). A new method of cryptography using Laplace transform. **International Journal of Mathematical Archive, 3(3), 1193-1197.**

[4] Panityakul, T., Bano, M., Shah, T.M. and Prangchumpol, D. An RGB Color Image Double Encryption Scheme, **International Journal of Mathematics and Computer Science, 17(2022), no. 1, –**

[5] Thinnukool, O., Panityakul, T. and Bano, M. Double Encryption Using Trigonometric Chaotic Map and XOR of an Image", **Computers, Materials & Continua vol. 69 no. 3, 2021** doi:10.32604/cmc.2021.019153

[6] Bano, M., Saleem, A., Shah, T.M., Panityakul, T. and Chinram, R., Extended Image Encryption with Markov processes in solutions images dynamical system of non-linear differential equations, **Journal of Mathematical and Computational Science, J. Math. Comput. Sci. 10(6), (2020).**

[7] Khan, A.A., Qiyas, M., Abdullah, S., Jianchao, L. and Bano, M. Analysis of Robot Selection Based on 2-Tuple Picture Fuzzy Linguistic Aggregation Operators, **Mathematics 2019, 7, 1000; doi:10.3390/math7101000**

[8] Huanhuan, J., Ashraf, S., Abdullah, S., Qiyas, M., Bano, M. and Shouzhen, Z., Linguistic Spherical Fuzzy Aggregation Operators and Their Applications in Multi-Attribute Decision Making Problems, **Mathematics 2019, 7, 413; doi:10.3390/math7050413**

[9] Bano, M., Shah, T, Talat, R. and Shah, T. M. Image reconstruction and text embedding using scan pattern with XOR in graph cut technique**. Journal of Intelligent & Fuzzy Systems. 33(2), 1097-1104 (2017).**

[10] Bano. M., Shah. T.M. and Shah. T. "Genetic Algorithm on Piecewise Linear Chaotic Map Bases Image Encryption". **Indian Journal of Science and Technology. 9(8), 2016.**

[11] Bano. M., Shah. T., Talat. R. and Shah. T.M. "Image reconstruction and text embedding using graph cut". **Science International. 28(2), 905-911 (2016).**

[12] Shabir. M., Jun. Y.B. and Bano. M. "On Prime Fuzzy Bi-ideals of semigroups", **Iranian Journal of fuzzy systems. 7(3), 115-128 (2010).**

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

[14] Qin. C., Zhou. Q., Cao. F., Dong. J. and Zhang. X. Flexible lossy compression for selective encrypted image with image in painting. **IEEE Trans. Circ. Syst. Video Technol. (2018)**

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

[16] Lingfeng. L. and Suoxia. M. "An image encryption algorithm based on baker map with varying parameter," **Multimedia Tools and Applications, 76(15), 16511-16527 (2017).**

[17] Duan. X., Liu. J. and Zhang. E. Efficient image encryption and compression based on a VAE-generative model. **J. Real-Time Image Process, 1–9 (2018).**