RESEARCH ARTICLE OPEN ACCESS

Secure Image Encryption Using Trigonometric Chaotic Maps and XOR Technique

Swaira Maryam[1], Gul Freen[2]
Mathematics, International Islamic University Islamabad H-10,
Pakistan
[1] Corresponding author:swairamaryam@gmail.com
[2]gul.phdma89@iiu.edu.pk

Abstract:

In the last few decades many image encryption strategies have been established out of which most have been shown to provide high security. Nevertheless, their processes are complicated, and their general speed is moderate to low, which makes these algorithms unsuitable for real-time applications. In an effort to mitigate this shortcoming, we introduce an improved new, fast and efficient image encryption approach called Trigonometric Chaotic Map. Unlike other method, this method uses the Trigonometric Chaotic Map that is comparatively easy and generates only a few random rows and columns at a time to save computation time. Also, the ongoing encryption process changes from the pixel to row and column levels that greatly increases the process speed. The current scheme of work observes a replacement-permutation network that improves security by performing a circular shift on the rows and columns, therefore breaking the very high dependency of pixel values adjacent to one another. Next, to enhance pixel values' confidentiality and avoid leakage of the data, the scheme employs XOR with modulo function. Security simulations and other detailed tests prove the high efficiency of this approach. The scheme has therefore the capabilities of achieving processing speeds in the range of real-time processing at 80 frames per second and at the same time providing very high levels of security for image encryption.

Keywords **— Cryptography, Chaotic Map, Encryption, NIST**

I. INTRODUCTION

Ever increasing multimedia and communications technologies have posed great questions on data security due to increased data capacity. The topic of this issue has been of interest among experts, researchers, and analysts in the field. However, simple text based encryption algorithms like the Advanced Encryption Standard (AES) [8], Data Encryption Standard (DES) [18] and RSA [20] are not good for image data security. The primary reason to be rooted in the nature of text and image data itself. Images are normally much bigger in size and are redundant and are normally highly correlated from pixel to pixel. Secondly, image decryption is normally done basing on what our eyes Eyes can distinguish, so a little distortion in the decrypted images is allowable. In light of these characteristics of digital images, many image encryption approaches have been developed such as the use of chaotic maps [17,18], DNA encoding [3, 5], quantum theory based approaches [2,17], scalable encoding[28] and the combined flexible compression with image imprinting [19]. These approaches are designed to address the known shortcomings of traditional forms of encryption to safely secure the image data [7]. Spearheading the research being done in this field of study is as a result of the increased innovations in encryption schemes for digital images.

Cryptography has effectively benefited from chaos theory because of its unique characteristics which

meet key characteristics of secure encryption. Some of these properties are: ergodicity, parameter and initial values dependence, no predictable nature and probabilistic nature [14, 22]. As a result, a number of investigations suggested image Security technique based on existing chaotic maps including Arnold cat map [2, 15], tent map [10, 13], sine map [9, 23] and logistic map [18, 19]. Current research has discredited new chaotic maps [5, 12] which has such benefits as wider chaotic region, higher ergodicity, higher unpredictability and more simple structures comparing to the conventional chaotic maps. Nevertheless, these benefits are not without compromise because these recently discovered chaotic maps are not yet widely used in cryptographic uses. Interestingly, most of the current image protection methods are based only on chaotic maps for producing multiple chaotic values corresponding to each pixel of plaintext image. This approach increases computational demand this results in high power consumption of the processor, and slow speeds in the encryption process. Due to this, such encryption schemes are unsuitable for real-time or continuous image processing; signifying the existence of opportunities for methods that meet these demands.

In this paper, a new efficient image encryption system is proposed that uses XOR operations and trigonometric map of chaos. The trigonometric chaotic map which is known as simple and strong chaotic system is defined by Orcan Alpar [12] and it has properties similar to logistic map. Nevertheless, the new discovered trigonometric map is more chaotic than the logistic map for a wider range of the chaotic boundary values, enlarges the critical area and increases the security level. The new proposed scheme brings a number of new concepts aimed to enhance the performance of the system and assure its security. This moves the processing unit from the pixel level to row/column level, and speeds up the encryption and decryption. In addition, the scheme uses the trigonometric chaotic map in the most efficient manner where only three rows and three columns of chaotic values are generated in each round of encryption completely in contrast to an image encryption rounds proposed by most of the a forenamed methods which are computationally expansive. A large number of performance and security evaluations shown in this paper clearly illustrate that the proposed scheme has very high performance and provides acceptable level of security. In particular, it can provide real time image processing with 80 fps for images of size 512×512, and the required level of security is comparable with the modern encryption methods. These attributes render the scheme highly appropriate for real-time image processing techniques and secure communications. Real-world applications of the suggested approach are related to securing satellite images in transmission, encrypting and decrypting images transmitted from remotely controlled drones, and securing stored images for real-time iris biometric recognition. The above use cases explain why the proposed scheme is flexible and performs well in meeting contemporary image encryption needs.

The primary contributions of this paper are as follows:

- A new high-security advance image encryption technique based on chaos is presented and the technique can process the images in real time with 80 frames per seconds.
- The Trigonometric chaotic map is used for the first time for image encryption and its efficiency and suitability is proved.
- The detailing use of the chaotic map is applied to developed the pseudo-random numbers of increased randomness in the fulfilment of augmenting the encryption process.
- The encryption framework alters from the operational mode of data pixel to the data row and then column, highly increasing the rate of encryption and decryption.

II. Image Encryption Based on the Trigonometric Chaotic Map

The traits of chaotic maps that are relevant to cryptographic applications are pseudo randomness, sensitivity to initial values as well as control parameters, non-predictability, and simplicity of implementation. These properties make chaotic maps to be widely used in the generation of chaotic

key streams, which play a crucial role in the secure image encryption. Nonetheless, many chaotic maps are not capable to be used in image transmission because of its limited range and instability. In this paper we propose a new technique of image encryption that uses Trigonometric Chaotic Map with XOR (TCMX). Properties of the TCM's are described and used as the basis for constructing an effective way of encrypting images. The outcomes of the exploratory analysis indicate that the TCM's yields high chaotic behaviour, s-unimodality and sensitive dependence on initial conditions. In addition, with the TCM's, the random key streams provide results on the NIST statistical test thus being suitable for use in cryptographic applications. The outcomes of the paper show that the new TCM based image encryption scheme can offer both the security and efficiency. Experimental outcomes performed on grayscale images show that the present method enhances the secure encryption along with a reduced processing time so it is an appropriate answer for real-time image encryption scheme.

III. QUICK SURVEY OF LITERATURE

An increased rate in multimedia technology allied to computer networks, and the use of cloud storages together with generation of enormous quantities of data bring about one of the best attributes of security, that of securing private and confidential information. In relation to the users' requirements, a security mechanism has to demonstrate high levels of protection while not having a negative impact on system functionality or ease of use. It has now been realized that image encryption has become a viable and popular approach in the protection of images while stored and transmitted. However, typical image characteristics as strong pixel correlation, high inequality coefficients, low pixel sensitivity, redundancy etc. show that traditional encryption technique can be ineffective to image encryption [30]. In this context, the usage of chaotic maps has received considerable attention because of their discrete nature, inherent random-like appearance, and simplicity of realization, dependence of system orbits on control parameters, initial conditions and unpredictability. The literature offers a vast number of chaotic maps compatible for image encryption with advantages and shortcomings of each have been earlier discussed. Some of these are the cross-chaotic map [13], convex sinusoidal map [8], parameter varying baker map [27], a sine and tent map combination [20] and generalized sine map [18], the generalized logistic map [26]. These chaotic maps have given a push towards the advancements of image encryption and each of these maps to some extent has its drawbacks in term of randomness, security and speed of encryption that is why this research field stays very active.

The logistic map that is known to the world as one of the most famous chaotic maps has some drawbacks. These are a small key space, easily guessable, a biased distribution of the iteration variable x, and comparatively low Lyapunov exponent [26], [24]. Putting together, these negative points reduce the strength and stability of numerous randomizing cryptosystems [31]. Moreover, many studies have pointed out that there are security flaws in many stochastic maps widely used in extensive existing investigations, including the logistic map, Mandelbrot map, and symmetric tent map. As noted in a variety of prior chaotic-based image encryption algorithms in the literature [19], [22], most of the researchers target a high extent of either efficiency or security while neglecting a trade-off between these two factors.

This chapter presents TCMX – a new one-parameter trigonometric map based chaotic map family known as the Trigonometric Chaotic Map with XOR. Key properties of the TCM are described and discussed in terms of extreme sensitivity to the initial conditions, chaos, s-unimodality and randomness. Based on these characteristics, an image encryption approach is presented to explore fully the inherent advantage of TCM. At last, some fundamental numerical tests related to statistical characteristics and the investigation of encryption capability of the proposed image encryption system are presented and discussed through software simulations to illustrate the feasibility and reliability of the scheme.

IV. THE TRIGONOMETRIC CHAOTIC MAP

Equation (1) is the mathematical model of the proposed TCM.

$$s_{n+1}= \begin{cases} \lambda s_n \left(\sin\left(\frac{\pi}{2}s_n\right) + \cos\left(\frac{\pi}{2}s_n\right)\right), & 0 \le s_n \le 0.5 \\ \lambda(1-s_n)\left(\sin\left(\frac{\pi}{2}(1-s_n)\right) + cos\left(\frac{\pi}{2}(1-s_n)\right)\right) & \\ \quad , 0.5 < s_n \le 1 & \end{cases} \quad (1)$$

Where $s_{n+1} \in [0, 1]$, λ represents the control parameter, and s_0 represents the initial condition.

A. Analysis of TCM Characteristics

In this section, some properties of the Trigonometric Chaotic Map (TCM) are described. Reviewed properties include chaotic dynamics, s-unimodality, changes that take place when there is a slight variation in the state of the system, and randomness. The discussion on the iterative behaviour of the TCM is shown in Fig.1. Where the value of iteration starts at Zero, then reaches the maximum value before reducing to Zero on the same cycle. The iteration function has only one peak hence showing the unimodality required for the TCM at $\lambda = 1.42$.

Further analysis is provided about the range of the λ, under which the TCM satisfies the unimodality property. For this analysis, the bifurcation diagram [29] is used as depicted in Fig.2 for the parameter λ in the range [1.3-1.55]. The bifurcation diagram also verifies that one of the requirements of the TCM, the unimodality characteristic of λ, holds for the λ values in the range between 1.3859 and 1.4424. These results indicate qualitative chaotic attributes of the TCM suitable for secure crypto applications due to sound chaotic virtues.

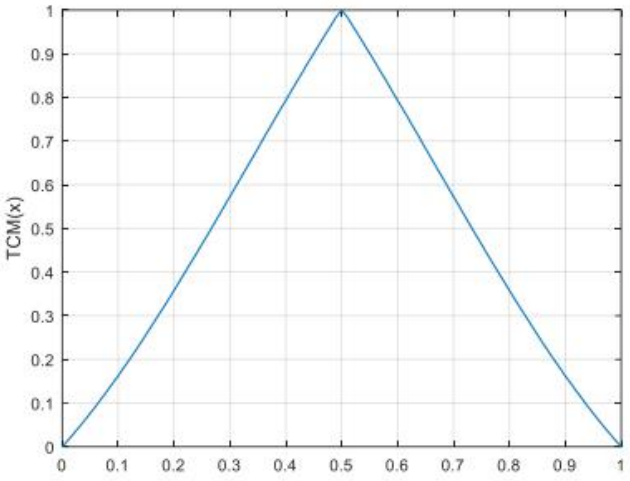

Fig.1: Iterative Function of the TCM at $\lambda = 1.42$

In this paper the existence of the Trigonometric Chaotic Map (TCM) is shown as well as analysing its chaotic behaviour through the Schwarzian derivative [4]. The Schwarzian derivative of TCM was given by the following mathematical representation in Equation 2. In Fig.3 we show the Schwarzian derivative of the TCM obtained through the numerical simulation for the control parameter λ equals 1.42 and the initial condition s_0 = 0.26 . Fig.3 shows that the Schwarzian derivative is negative over the whole interval. Thus, it can be concluded that TCM is chaotic at the given initial condition and the value of control parameter. As this result verifies that the TCM is appropriate to use for applications that necessitate solid chaotic form, it clearly establishes how useful this method is in chaotic research.

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

Furthermore, the selected control parameter and initial condition of this paper are responsive to the s-unimodality property of TCM owing to its robust chaotic aspect alongside with unimodal features. Especially worthy of further research is the TCM's ability to respond to small changes in the initial condition.

This sensitivity is showed in the Fig.4, which illustrates two sequences obtained by computing (1). In each iteration step, the two sequences are altogether far apart and complicated compared with the previous step. This behaviour illustrates the

high degree of responsiveness of the TCM to variations in the initial condition, which is currently a requirement for its use in secure cryptographic systems.

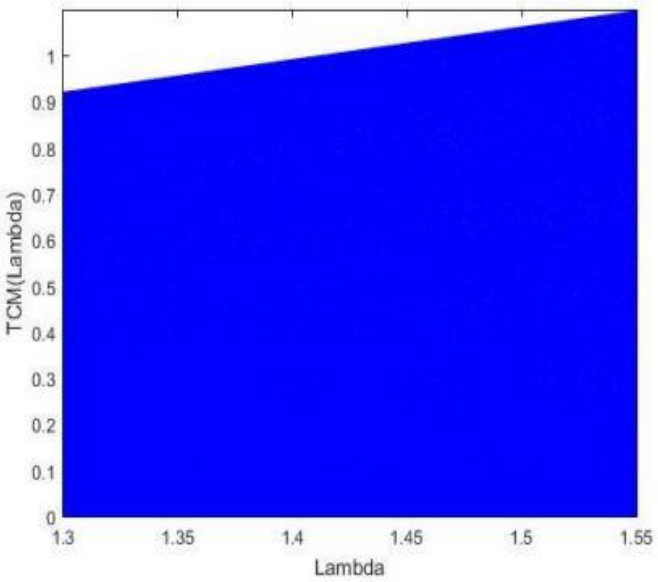

Fig.2: Bifurcation Diagram of the TCM at $\lambda \in [1.3, 1.55]$

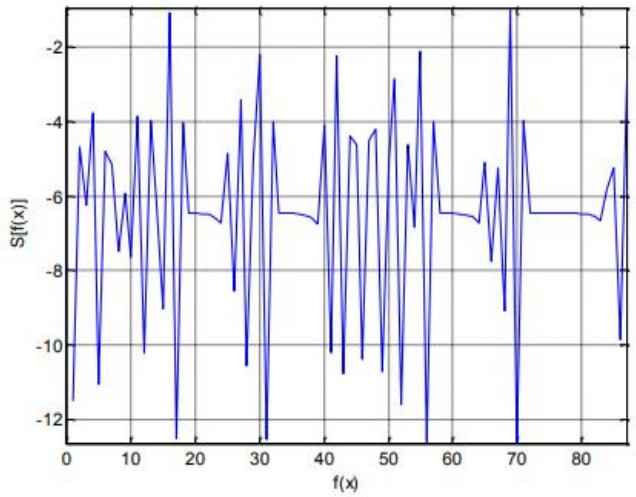

Fig.3: Schwarzian Derivative of the TCM at $\lambda = 1.42$

As the study also aims to examine the behaviour of the TCM, the value of the Lyapunov exponent is utilized for that purpose in Equation (3). Derivative of condition (1) is given in (4). The Lyapunov spectrum of the TCM is illustrated in Fig.5 for the control parameter range $\lambda \in [1, 1.6]$. According to the literature, a chaotic map demonstrates chaotic behaviour when its Lyapunov exponent lies within the range [0, 0.69]. It can also be appreciated from the graphical representation of Fig.5 that for $\lambda \in [1, 1.466]$ the TCM shows chaotic behaviour.

The results produced from the bifurcation diagram and Lyapunov exponent corresponds with the chaotic attributes of TCM and s-unimodality in the range of $\lambda \in [1.3859, 1.4424]$. On the other hand, the logistic map and tent map introduce chaotic and satisfy s-unimodality property of $\lambda \in [3.96, 4]$ and $\lambda \in (1.999, 2)$, respectively. Indeed, the present study shows that the TCM is capable of producing a wider spectrum of chaotic behaviour than both the logistic and tent mappings, which means it is better suited for heavily utilized environments that necessitate reliable chaotic characteristics.

$$\lambda_{LE}(s_0) = \lim_{n\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln|f'(s_n, \lambda)| \qquad (3)$$

The final characteristic explored here is random and is inherent to deciding the appropriateness of TCM for cryptographic uses. A secure key stream generator must have no detectable periodicities and therefore no tendencies toward being biased. In order to determine whether the key streams produced by the TCM output data that behave in a random-like manner, the NIST statistical measure is used [10].

The NIST statistical analysis suite is composed of fifteen statistical measures intended for finding out diverse forms of non-randomness in binary sequences. First, as the preliminary step, the iteration of the TCM are converted to the binarization form, depicted by the equation (4). These binary sequences are then put through the battery of tests from NIST conveyor to determine compliance in terms of randomness as an indicator of suitability in desired cryptographic TCM application.

$$\beta_i = \begin{cases} 0, & 0 \le s_i < 0.5 \\ 1, & 1 \ge s_i \ge 0.5 \end{cases} \qquad (4)$$

All NIST test is performed at a 1 % significance level ($\alpha = 0.01$), this means that it is anticipated that one sequence in a hundred will be erroneously rejected. For each of the employed statistical tests, a p-value is implying that one sequence out of every 100 is expected to be rejected by chance. It is concluded that a sequence is random with the significance level of 1% if p -value constantly

exceeds the selection criteria. On the other hand, if the p -value that we get in the sequence is less than or equal less is equal to α ($p \leqslant \alpha$), then sequence is said to be rejected as random. Ted to be rejected by chance. For each statistical test, a p -value is computed. A sequence is identified as random with 99% confidence if the p -value surpasses the significance level. Conversely, if the p -value is less than or equal to the significance level, the sequence is classified as non-random and subsequently rejected. These criteria afford a formal means by which the randomness of the key streams produced by the Trigonometric Chaotic Map (TCM) may be assessed and ensured.

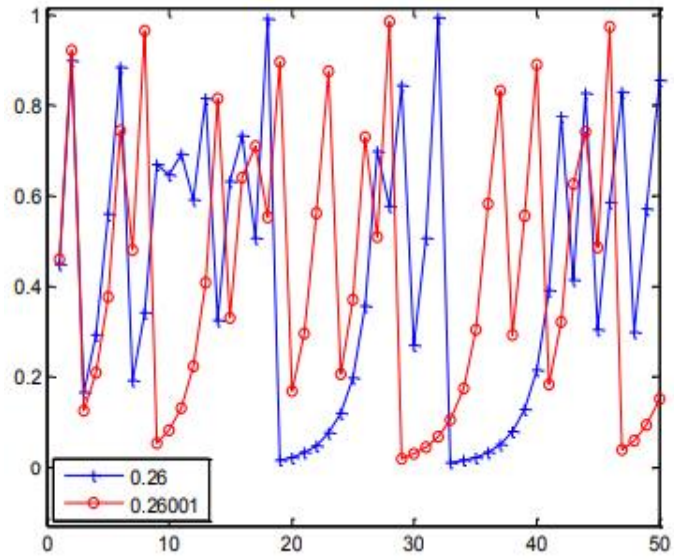

Fig.4: 'Two Sequences Generated with (s_0 , λ) = (0.26, 1.42), Represented by Squares, and (s_0 , λ) = (0.26001, 1.42), Represented by Circles'

Table I to III displays an analysis accomplished through the NIST statistical test suits on 100, 200000 bits string based on TCM, Tent Map and Logistic Map. For each test, p-values were determined whereas for each of the key streams, the percentage of condition p-value greater than α was noted.

Table I shows that TCM has better performance than Tent Map and Logistic Map to generate these key stream with a higher number of p-values of p-value $\geqslant$ 0.01. The chi-square test further intensifies this evidenced by the TCM and Tent Map which gave p-values above the significance level α = 0.01. But the logistic map got failed in three specific tests, those are, longest run of one's, run, block frequency test highlighting that the Logistic Map possesses weaker randomness characteristics.

P-values of all three maps were obtained falling between zero and one and were close to each other. Fortunately, from the simulation results of TCM and Tent Map, the significance value p of the key streams, derived were generally greater than 0.01 which indicates with more than 99 percent confidence that the obtained key streams displayed random like behaviour. These results help to confirm that the TCM is superior at creating these random key streams, and as a result is ideal for cryptographic use.

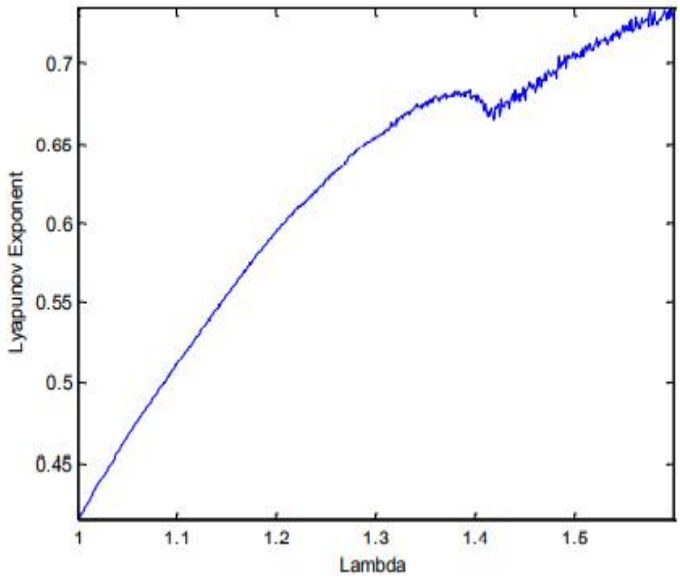

Fig.5: Lyapunov Exponent of the TCM at $\lambda \in [1, 1.6]$

V. PROPOSED METHOD FOR IMAGE ENCRYPTION

The proposed image encryption strategy is summarized as follows. Without loss of generality, dimension of the image encryption I are assumed to be $M \times N$.

1. The original image is resized to a fixed dimension of 256 × 256 pixels to standardize the encryption process.
2. Any image with the identical dimensions ($M \times N$) as the original image is generated.
3. Both the authentic and randomly generated images are divided into square blocks, each of size $m \times m$ pixels. The block size m is determined using Equation (5):

$$m = \frac{\sqrt{M \times N}}{r^2} \quad (5)$$

An important part of both encoding and the secret key is the parameter r, together with the control boundary and the initial condition of the Trigonometric Chaotic Map (TCM).

4. The following steps are performed on each square block of the initial and generated images:

- The square block of the same size of the first and randomly selected images is then vectorized. To obtain a new row vector we perform an XOR operation between the row vector of the original image and the row vector of a random image.
- By substituting as in (1), a vector $[1, m \times m]$ is formed in order to produce random numbers.
- The obtained pseudorandom numbers are used as indices of locations of pixels in order to shuffle these locations in the row vector that increases confusion.
- The new values of the pixel intensity of the rearranged row vector is calculated by the help of as in (6). This modification one again tends to strengthen the encryption by adding further randomization to the pixel intensity range.

$$K = \sin(K + b) + K \quad (6)$$

Where K is a key stream derived from (1), and b is the resultant row vector the original row vector from previous step is XOR with the random row vector.

- The modified row vector can then be placed in a square block of $m \times m$ pixels thus can create a segment of the encrypted image.

5. Lastly, in accordance to Equation (6), it further modifies pixel intensity values of the encrypted image. This added measure further improves the security of the proposed encryption procedure, because the pixel intensity values undergo one more level of non-linear transformation.

These procedures enable the enhancement of the strength of the encryption method withstanding several cryptographic attacks but still being efficient.

VI. EXPERIMENTAL RESULTS

Hence two test images namely Lena and Cameraman images were used to test the efficiency of the proposed image encryption technique. The encryption process was done in MATLAB and the Lena image was used for the purpose of this study. Fig. 6 shows the Lena image used earlier in this text and Fig.7 depicts its histogram. Histogram of the original image is depicted in Fig.7 the proposed technique, the distribution of pixel intensity values does not cover the complete range of intensities; most of the data points are in the mid-tone densities. The above work of encryption was done using the parameter, r = 4 and this gave the resulting blocks of size, 16× 16 pixels. The encryption process was implemented in MATLAB, with the Lena image serving as the reference image for this study. Fig.6 presents the original Lena image, as used in earlier sections, while Fig.7 illustrates its histogram. The histogram of the original image, shown in Fig.7, reveals that the pixel intensity values are not evenly distributed across the entire range, with most values concentrated around mid-tone densities.

The encryption process was carried out with a parameter r = 4, resulting in square blocks of 16× 16 pixels. The encrypted Lena image that is produced using this method is shown in Fig.8. By observing the encrypted image the effect of embedding the information is clearly seen as the actual visual content of the image is completely distorted. Besides, the histogram of the exhibited encrypted image, as shown in Fig. 9, reveals that the pixel intensity is semi scale uniformly distributed.

The obtained semi- uniform histogram distribution in present work analytically proves the

effectiveness of the proposed technique to counter histograms based attacks and gives reliable evidence to supports the method for secure image encryption. For the purpose of testing its ability to resist brute-force attacks, the proposed encryption technique is examined. By definition, brute-force attack tactics involve the process of scanning all the possible values of secret key parameters for the purpose of decrypting an encoded image.

From experimental results it is observed that the value x_0, λ and K has to be fixed up to $10^{18}, 10^{17}$ 10^{16} respectively in order for the decrypted image to be a replica of the original image and the encrypted image respectively. As such, the proposed encryption method receives the complexity of O (2^{169}). Based on the cryptographic measures, any encryption algorithm must be cryptographically secure with a complexity level higher than (2^{128}), in a bid to withstand brute force attack [14]. This analysis shows the efficiency and the high degree of safety of the presented encryption method.

Fig.6: Lyapunov Exponent of the TCM for $\lambda \in [1, 1.6]$

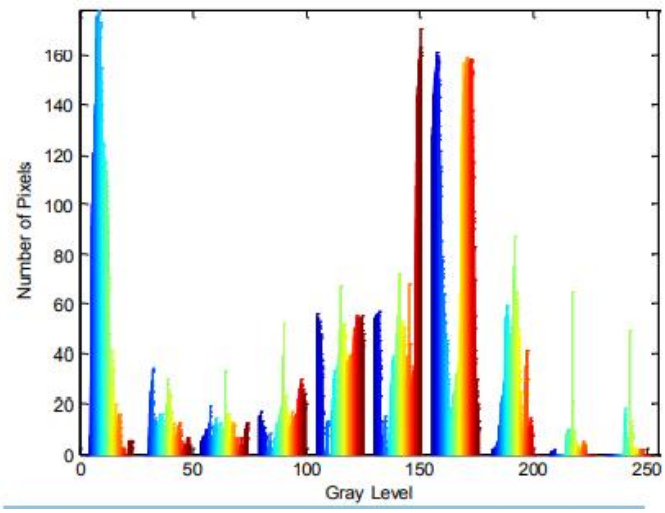

Fig.7: Histogram of the Lena Image Shown in Fig.6

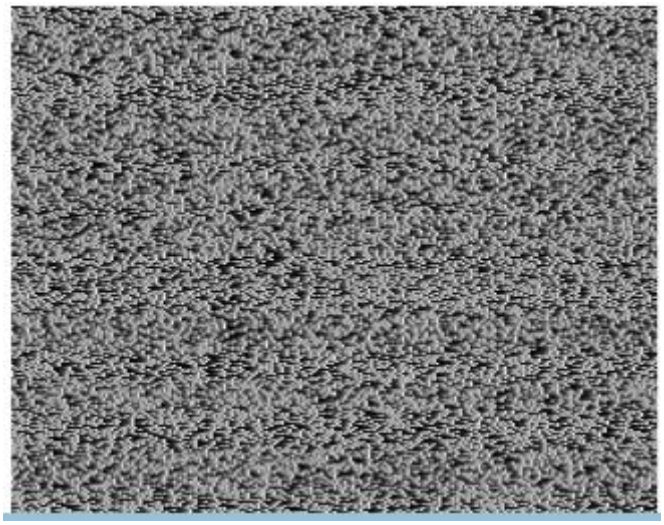

Fig .8: Encrypted image using encryption method

The work examines how susceptible the encryption method is to the characteristic of having a high correlation between consecutive pixels in the image. Thus, the horizontal, vertical and diagonal relationship between the two successive pixels in an image is calculated with the help of Equation (7). This evaluation suggests how the proposed encryption technique is able to degrade the predetermined innate relationship of adjacent pixels, which is helpful in determining the efficiency of encrypting image algorithms.

$$r = \frac{2\sum_{i=1}^{2}(x_i,y_i) - \sum_{i=1}^{2} x_i \sum_{i=1}^{2} y_i}{\sqrt{(2\sum_{i=1}^{2} {x_i}^2 - (\sum_{i=1}^{2} x_i)^2)(2\sum_{i=1}^{2} {y_i}^2 - (\sum_{i=1}^{2} y_i)^2)}} \quad (7)$$

In the encryption method (x_0, y_0), mean two pixel intensity levels randomly chosen from the adjacent pixels to make the system more secure. Filtering a total of 1000 consecutive pixels, the correlation coefficients for the vertical, the horizontal, and the diagonal pixel displacement were computed. Comparisons of the encryption performance of the proposed TCM with those of the other chaotic maps such as LM, TM, and NCA were made using Equations (9–11). From Table IV, these results show that although the pixels in the original images were strongly correlated, the encrypted images showed far less pixel correlation.

As we had expected, our statistical comparison shown that the proposed TCM-based encryption method yielded the smallest mean value of pierce's among all the computed methods. Furthermore, entropy analysis was conducted to analyse the amount of randomness of the encrypted images. Table IV below shows the entropy of the original image was low, which means that there is order in the placement of objects with relation to other objects in the image. But, the entropy values of the encrypted images, obtained through the proposed scheme were nearly to the ideal value of eight. While the encryption technique that used the Tent Map achieved the highest entropy, the entropy from the TCM based method was as close to ideal as can be considered.

These results reaffirm the suitability of the developed TCM-based encryption technique in providing high security against Entropy-based attack. The enhanced permutation and substitution features of the developed TCM-based scheme are evidenced by the following characteristics of the histogram pattern: it is at least semi- uniform for different benchmark images Other statistical measures comparing the encrypted image from uncompressed images comprise of low statistical correlation coefficients and high entropy values. For decryption, the reverse process discussed in section IV is followed in detail to gain a perfect image of the images to be transmitted.

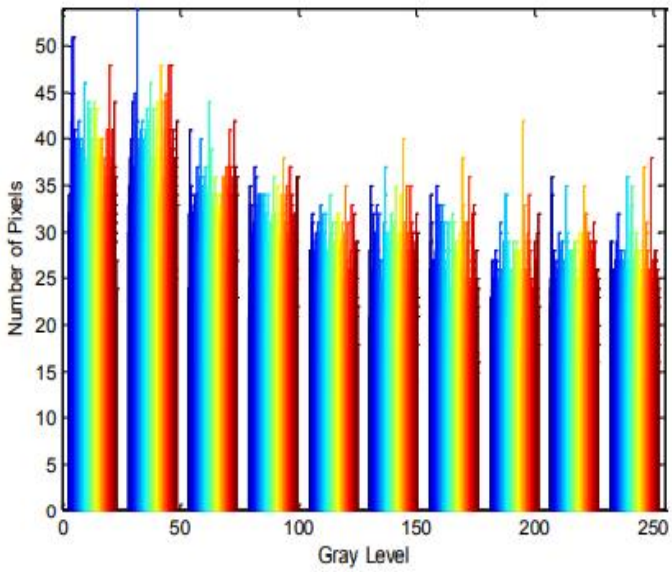

Fig.9: Histogram of the Encrypted Image Shown in Fig.8

$$s_{n+1} = \lambda\, s_n(1 - s_n) \qquad (8)$$

$$s_{n+1} = (1 - \lambda^{-4}) \cot\left(\frac{\alpha}{1+\lambda}\right)\left(1+\frac{1}{\lambda}\right) \tan(\alpha s_n)(1 - s_n)^{\lambda} \qquad (9)$$

$$S_{n+1} = \begin{cases} \lambda s_n, & s_n < 0.5 \\ \lambda(1 - s_n), & s_n \geq 0.5 \end{cases} \qquad (10)$$

This work presents a new one-dimensional Trigonometric Chaotic Map (TCM) suitable for cryptographic uses. These experimental results confirm the theoretical findings and show that the TCM is s-unimodal, has a large range of chaotic behaviour, and is sensitive to the small initial perturbations. Moreover, TCM's key streams from all registers pass the NIST statistical test suite that established their appropriateness for use in cryptography. The proposed image encryption strategy, based on the TCM, consists of two primary stages: Two representatives of micro operations are pixel substitution and pixel permutation. In this stage, image pixel positions are changed for security improvement purposes. Experimental results prove the insensitivity of the proposed strategy to entropy and brute force attacks. The results also confirm that the substitution and permutation capabilities of the encryption scheme

are optimal and safeguard the cryptographic system against key attacks.

Further research should be conducted in order to assess the security of the proposed encryption against other complex attacks like prevent replay attack and Real Man in the Middle attack and make the proposed method secure for practical cryptographic applications.

Table I
'NIST Statistical Test Results for 100 Key Streams of 200,000 Bits Each, Generated by the TCM with Control Parameter λ = 1.42 and a Randomly Chosen Initial Value'

Statistical Measure	p-value	Proportion
Frequency Analysis	0.096568	97%
Block Frequency Analysis	0.203319	99%
Forward Cumulative Sums Analysis	0.122268	98%
Reverse Cumulative Sums Analysis	0.149716	96%
Random Excursions(x=1)	0.888728	100%
Random Excursions Variant (x=8)	0.973220	100%
Rank Analysis	0.682537	99%
Non-Periodic Templates Matching	0.419021	98%
Overlapping Templates Matching	0.565544	97%
Entropy Approximation Analysis	0.291687	98%
Runs Analysis	0.997743	98%
Longest runs of one's Analysis	0.714000	99%
Linear Complexity (substring length = 500)	0.934538	94%
Serial Test 1	0.161557	97%
Serial Test 2	0.997119	99%

Table II
'NIST Statistical Test Results for 100 Key Streams of 200,000 Bits Each, Generated by the Tent Map with Control Parameter λ = 1.9999 and a Randomly Chosen Initial Value'

Statistical Measure	p-value	Proportion
Frequency Analysis	0.137282	98%
Block Frequency Analysis	0.108791	96%
Forward Cumulative Sums Analysis	0.262249	97%
Reverse Cumulative Sums Analysis	0.122325	94%
Random Excursions(x=1)	0.035174	100%
Random Excursions Variant (x=8)	0.739918	98%
Rank Analysis	0.953118	99%
Non-Periodic Templates Matching	0.555937	98%
Overlapping Templates Matching	0.31444	99%
Entropy Approximation Analysis	0.213309	98%
Runs Analysis	0.383827	100%
Longest runs of one's Analysis	0.675450	98%
Linear Complexity (substring length = 500)	0.145326	100%
Serial Test 1	0.534146	98%
Serial Test 2	0.115387	97%

Table III
'NIST Statistical Test Results for 100 Key Streams of 200,000 Bits Each, Generated by the Logistic Map with Control Parameter λ = 1.9999 and a Randomly Chosen Initial Value' (4)

Statistical Measure	p-value	Proportion
Frequency Analysis	0.419021	100%
Block Frequency Analysis	0.003201	91%
Forward Cumulative Sums Analysis	0.911413	100%
Reverse Cumulative Sums Analysis	0.275709	100%
Random Excursions(x=1)	0.534146	100%
Random Excursions Variant (x=8)	0.213309	100%
Rank Analysis	0.955835	98%
Non-Periodic Templates Matching	0.798139	100%
Overlapping Templates Matching	0.145326	96%
Entropy Approximation Analysis	0.026948	97%
Runs Analysis	0.00000	74%
Longest runs of one's Analysis	0.000954	94%
Linear Complexity (substring length = 500)	0.494392	100%
Serial Test 1	0.759756	100%
Serial Test 2	0.153763	99%

Table IV
'Correlation Analysis of 1,000 Randomly Selected Neighbouring Pixels from Original and Encrypted Images'

	Original image	LM-Based encrypted image λ = 3.97	TM-Based encrypted image λ = 1.9999	TCM-Based encrypted image λ = 1.39	NCA-Based encrypted image λ = 3.5
Average correlation	0.9320	0.0973	0.0349	0.0105	0.0766
Diagonal correlation	0.9133	0.0395	0.0421	0.0482	0.0355
Vertical correlation	0.9764	0.023	0.0396	0.0503	0.0371
Horizontal Correlation	0.9406	0.2304	0.0346	0.0331	0.1773
Entropy	7.0097	7.7496	7.988	7.8772	7.0707

VII. CONCLUSIONS

In this paper, an anti-attack image encryption system is introduced the Random Image XOR TCM system that is a combination of a random image and the Trigonometric Chaotic Map to increase the level of security. An arbitrary image and the initial row vector of the chaotic map are employed to strengthen the encryption mechanism to be less susceptible to attacks. The encryption scheme uses confusion and diffusion in each row of vectors. In particular, XOR operation helps to form a row vector, and TCM – to produce the encrypted image. Subsequently, the security of the proposed algorithm is thoroughly analysed using benchmark cryptographic tests were the outcomes are also presented and discussed to show the viability of the algorithm.

REFERENCES

1. *M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Dandache, "Robust chaotic key stream generator for real-time image encryption," J. Real-Time Image Process., vol. 8, no. 3, pp. 297–306, 2013.*
2. *G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons Fractals, vol. 21, no. 3, pp. 749–761, 2004.*
3. *G. C., H. Kai, Z. Yizhi, Z. Jun, and Z. Xing, "Chaotic image encryption based on running-key related to plaintext," Sci. World J., vol. 2014, no. 1, p. 490179, 2014.*
4. *Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos-based S-Box," Chaos Solitons Fractals, vol. 95, pp. 92–101, 2017.*
5. *S. Dadras, H. R. Momeni, and G. Qi, "Analysis of a new 3D smooth autonomous system with different wing chaotic attractors and transient chaos," Nonlinear Dyn., vol. 62, no. 1–2, pp. 391–405, 2010.*
6. *D. Arroyo, J. Amigó, S. Li, and G. Alvarez, "On the inadequacy of unimodal maps for cryptographic applications," in Proc. 11th Spanish Meeting on Cryptology and Information Security, pp. 37–42, 2010.*
7. *X. Duan, J. Liu, and E. Zhang, "Efficient image encryption and compression based on a VAE generative model," J. Real-Time Image Process., pp. 1–9, 2018.*
8. *N. I. S. T. FIPS-PUB, "Advanced encryption standard (AES)," Federal Inf. Process. Std. Publ., vol. 197, no. 441, p. 0311, 2001.*
9. *Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," Inf. Sci., vol. 297, pp. 80–94, 2015.*
10. *C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dyn., vol. 87, no. 1, pp. 127–133, 2017.*
11. *F. Li, H. Wu, G. Zhou, and W. Wei, "Robust real-time image encryption with aperiodic chaotic map and random-cycling bit shift," J. Real-Time Image Process., pp. 1–16, 2018.*
12. *L. Lingfeng and M. Suoxia, "An image encryption algorithm based on baker map with varying parameter," Multimedia Tools Appl., vol. 76, no. 15, pp. 16511–16527, 2017.*
13. *Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," Nonlinear Dyn., vol. 83, no. 4, pp. 1–18, 2015.*
14. *J. Meng and X. Wang, "Generalized projective synchronization of a class of delayed neural networks," Mod. Phys. Lett. B, vol. 22, no. 3, pp. 181–190, 2008.*
15. *F. Musanna and S. Kumar, "A novel fractional order chaos-based image encryption using Fisher Yates algorithm and 3D cat map," Multimed. Tools Appl., 2018.*
16. *H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," Eur. Phys. J. Plus, vol. 133, no. 1, p. 6, 2018.*
17. *P. Glendinning, Stability, Instability, and Chaos, 1st ed. Cambridge, UK: Cambridge University Press, 1994.*
18. *FIPS PUB 46-3, "Data encryption standard (DES)," Natl. Inst. Std. Technol., vol. 25, no. 10, pp. 1–22, 1999.*
19. *C. Qin, Q. Zhou, F. Cao, J. Dong, and X. Zhang, "Flexible lossy compression for selective encrypted image with image inpainting," IEEE Trans. Circ. Syst. Video Technol., 2018.*
20. *R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.*
21. *L. Sui, K. Duan, J. Liang, and X. Hei, "Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps," Opt. Express, vol. 22, no. 9, pp. 10605–10621, 2014.*
22. *X. Wang, J. Zhao, and Z. Zhang, "A chaotic cryptosystem based on multi-one-dimensional maps," Mod. Phys. Lett. B, vol. 23, no. 2, pp. 183–189, 2009.*
23. *J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-sine map and DNA approach," Signal Process., 2018.*
24. *Y.-G. Yang, J. Xia, X. Jia, and H. Zhang, "Novel image encryption/decryption based on quantum Fourier transform and double phase encoding," Quantum Inf. Process., vol. 12, no. 11, pp. 3477–3493, 2013.*
25. *Y.-G. Yang, J. Tian, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," Inf. Sci., vol. 345, pp. 257–270, 2016.*

26. *Q. Zhang, X. Xue, and X. Wei, "A novel image encryption algorithm based on DNA subsequence operation," Sci. World J., pp. 1–10, 2012.*

27. *Q. Zhang, S. Zhou, and X. Wei, "An efficient approach for DNA fractal-based image encryption," Appl. Math. Inf. Sci., vol. 5, no. 3, pp. 445–459, 2011.*

28. *X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Image Process., vol. 21, no. 6, pp. 3108–3114, 2012.*

29. *Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," Inf. Sci., vol. 450, pp. 361–377, 2018.*

30. *P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," Multimed. Tools Appl., vol. 75, no. 11, pp. 6303–6319, 2016.*

31. *R.-G. Zhou, W. Qian, M.-Q. Zhang, and C.-Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," Int. J. Theor. Phys., vol. 52, no. 6, pp. 1802–1817, 2013.*