Original Article

https://napass.org.ng

APPLICATION OF A MODIFIED LOGISTIC MAP

Emmanuel O. Ejembi

Mathematics/Computer Science Department, Rev. Fr. Moses Orshio Adasu University, Makurdi

Abstract

The rapid expansion of digital communications and the internet has led to an increased need for robust encryption method to secure sensitive information, especially in images. Encryption of sensitive images in this modern age of technology has become necessary for ensuring that such images sent via the insecure public network called the internet are protected from attacks. In this research work, a modified one-dimensional logistic map for encrypting images is proposed and its properties are investigated. The modified logistic map incorporates the hyperbolic cosine function $\cosh(x)$ to enhance the complexity and versatility of the map, resulting in a broader range of dynamic behaviours, including chaos, which was confirmed through bifurcation analysis and Lyapunov exponent calculations. The proposed scheme was implemented and tested on standard grayscale images. The results of the experimental, statistical analysis and key sensitivity tests show that the proposed scheme provides an efficient and secure way for real-time image encryption and transmission. The performance evaluation using correlation coefficient analysis, histogram uniformity, confirmed that the encryption scheme successfully obscured the original image features and introduced strong diffusion and confusion properties, both of which are essential for resisting statistical and differential attacks.

KEYWORDS: Encryption, Decryption, Chaos, Cryptography and Images.

OPEN ACCESS

Correspondence:

E-mail:
ejembi1@gmail.com
Phone:
(+234) 8038985556

Specialty Section;This article was submitted to Sciences a section of NAPAS.

Citation: *Emmanuel O. Ejembi (2025) Application of a Modified Logistic Map*

Effective Date: Vol.8(1), 150-174

Publisher:cPrint,Nig.Ltd
Email:cprintpublisher@gmail.com

INTRODUCTION

Computer networks are often used for the transmission of images and other multimedia assets. Information security is jeopardized when it is transmitted over untrusted networks. According to Forouzan (2010) and Huang et al. (2012), for instance, photos end up in the hands of unauthorized third parties during communication due to persistent hacking attempts. These third parties may benefit from or alter the images without the recipient's knowledge. A crucial concern is the security of information that is transferred. Image encryption is not a good fit for conventional encryption methods like Rivest Shamir Adleman (RSA), Digital Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA). Because of the significant correlation between pixels in these encryption techniques, they need a lot of processing power and time. The scatter and disorder properties of the chaotic system have been applied to encryption and security communication by a small number of researchers (Wu et al., 2019; Turk et al., 2016; Gao et al., 2016), but they have not been applied to the encryption of digital images. The chaotic one-dimensional logistic map is a quick and easy way to encrypt images, however it cannot offer enough security. To improve communication security, the logistic map is modified into a one-dimensional hyperbolic chaotic system.

RELATED WORKS

Cryptography and Image Encryption

The security of digital images is attracting much attention nowadays and many image encryption algorithms have been proposed by different authors (Rajput and Gulve, 2014). According to Amber (2015) chaotic cryptography pronounces the use of chaos theory in specific physical dynamical systems working in chaotic system as a measure of communication techniques and computational algorithms to accomplish dissimilar cryptographic tasks in a cryptographic system. Reviewing some recent work on chaos – based cryptography, the researcher discovered that cryptographic methodologies are critically important for storage of secured media content and transmission over exposed systems, for example, the web. For high security, encryption is one of the approaches to guard the information from leakage. Image encryption is transformation of image to an inaccurate form so that it can be secured from unauthorized users (Rhee, 2003 and Ramadan *et al.,* 2016).

Exploring application of encryption in time samples pattern, the researcher recommended a secured approach to code input signals by introducing a new encryption algorithm. The algorithm mechanism is such that the transmitter, an input signal was received and coded into a lengthier series of numbers. At the receiver, the coded signal by the transmitter was received and changed back into its original values. This was done based on the idea that the hidden input signal samples using a specific pattern, could only be recoverable by a trusted receiver (Sneyers, 1997and Kumar, *et al.,* 2015). Fu *et al.* (2012) observed that Chaos-based image cipher has been widely investigated over the last decade or so to meet the increasing demand for real-time secure image transmission over public networks. Shah and Saxena (2011) proposed an improved diffusion strategy to promote the efficiency of the most widely investigated permutation-diffusion type image cipher. By using the novel bidirectional diffusion strategy, the spreading process was significantly accelerated and hence the same level of security was achieved with fewer overall encryption rounds. Moreover, to further enhance the security of the cryptosystem, a plaintext related chaotic orbit turbulence mechanism was introduced in diffusion procedure by perturbing the control parameter of the employed chaotic system according to the cipherpixel. Extensive cryptanalysis has been performed on the proposed scheme using differential analysis, key space analysis, various statistical analyses and key sensitivity analysis. Results of their research indicated that the new scheme was a satisfactory security level with a low computational complexity, which renders it a good candidate

for real-time secure image transmission application.

A system for efficient image encryptionthen-compression was designed by Nimbokar *et al.* (2014). Image encryption has to be conducted prior to image compression. The researchers considered how to design a pair of image encryption and compression algorithms such that compressing encrypted images can still be efficiently performed. The work introduced a highly efficient image encryption-then compression (ETC) system. The proposed image encryption scheme operated in the prediction error domain is able to provide a reasonably high level of security. More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency.

An efficient, secure color image coder based on color Set Partitioning in Hierarchical Trees (C-SPTHT) compression and partial encryption was presented by Karl *et al.* (2005). The use of a stream cipher and encryption of a small number of bits keeps computational demands at a minimum and makes the technique suitable for hardware implementation (Pritchard, 1996). By varying k, the level of confidentiality vs processing overhead can be controlled. It was found that using k = 2 achieved an adequate level of security for test images coded at 0.8 bits per pixel (bpp), resulting in an average of only 0.33% of the coded image been encrypted (Amig *et al.*, 2015).

Aljazaery (2013) developed a new method to encrypt the signals with one dimension and images (monochrome or color images) in a time more less than if these signals and images are encrypted with their original sizes. This method depends on extracting the important features which are distinguished these signals and images and then discarding them. The next step is encrypting the lowest dimensions of these data. Discrete Wavelet transform (DWT) is used as a feature extraction because it is a powerful tool of signal processing for its multiresolutional possibilities Xiang *et al*. (2008). The chosen data is encrypted with one of conventional cryptographic algorithm (Permutation algorithm) after shrinking its dimension using suitable encryption key. The encrypted data was 100% unrecognized, besides, the decryption algorithm returned the encrypted data to its original dimension efficiently.

Image applications have been increasing in recent years. According to Gotz *et al*. (1997) encryption is used to provide the security needed for image applications. Shah and Saxena (2011) in their paper classified various image encryption schemes and analyzed them with respect to various parameters like tenability, visual degradation, compression friendliness, format compliance, encryption ratio, speed and cryptographic security. Kartalopoulos (2008) observed that multimedia is one of the most popular data shared in the Web, and the protection of it via encryption techniques is of vast interest.

Schimtz (2001) proposed a secure and computationally feasible algorithm called Optimized Multiple Huffman Tables (OMHT) technique. OMHT depends on using statisticalmodel-based compression method to generate different tables from the same data type of images or video to be encrypted leading to increase compression efficiency and security of the used tables. A systematic study on how to strategically integrate different atomic operations to build a multimedia encryption system was presented. The resulting system can provide superior performance over other techniques by both its generic encryption and its simple adaptation to multimedia in terms of a joint consideration of security, and bit rate overhead. The effectiveness and robustness of this scheme was verified by measuring its security strength and comparing its computational cost against other techniques. The proposed technique guarantees security and fastness without noticeable increase in encoding image size (El-Said *et al.*, 2011).

The need of exchanging messages and secretly over unsecure networks promoted the creation of cryptosystems to enable receivers to interpret the exchanged information (Dachselt and Schwarz, 2001). In the presentation of Hashim and Neamaa (2014), a particular public key cryptosystem called the ElGamal Cryptosystem was considered with the help of MATLAB program used over images. Since the ElGamal cryptosystem over a primitive root of a large prime was used in messages encrypted in the free GNU Privacy Guard software, recent versions of Pretty Good Privacy (PGP), and other cryptosystems. The work shows a modification of this cryptosystem by applying it over gray and color images. That would be by transforming an image into its corresponding matrix using MATLAB program, then applying the encryption and decryption algorithms over it. Actually, this modification gives one of the best image encryptions that have been used since the encryption procedure over any image goes smoothly and transfers the original image to completely undefined image which makes this cryptosystem really secured and successful over image encryption. As well as, the decryption procedure of the encrypted image works very well since it transfers undefined image to its original. Therefore, this new modification can make the cryptosystem of images more immune against some future attacks since breaking this cryptosystem depends on solving the discrete logarithm problem which is really impossible with large prime numbers (de Oliveira and Sobottka, 2008; Bertuglia, 2005).

Vector Quantization (VQ) is an efficient technique for image encryption (Chen and Chang, 1997). Its basic idea is derived from Shannon's rate-distortion theory, which states that the better performance of an image compression is always achieved by coding image vectors instead of scalar (Guan and Guan, 2005). There are two advantages of using VQ for image compression. One is that the required bit rate of VQ is small. Since VQ compresses the original image into a set of indices in the codebook, we can save a lot of storage. The other is that to encrypt the codebook. The set of indices on the codebook is transmitted in plaintext form (Kanso and Smaoui, 2009).

Shannon proposed two basic techniques for obscuring the redundancies in plaintext message: diffusion and confusion involves many substitutions into the relationship between the plaintext and the ciphertext (Kocarev and Lian, 2011). This frustrates the attempts to study the ciphertext looking for redundancies and statistical patterns. Diffusion involves many transformations (or permutations) to dissipate the redundancies of the plaintext by spreading it out over the ciphertext. In addition to confusion and diffusion techniques, we also use some number theorems for our new image cryptosystem.

The new cryptosystem consists of the following three basic phases: encryption, transmission and decryption phases. In the encryption phase, we first apply VQ to compress our original image into a set of indices. Next, we diffuse and confuse the codebook, and encrypt these parameters of the codebook by a symmetric cryptosystem. In transmission phase, our scheme sends the set of indices and the above encrypted data of the codebook by a public channel. The scheme also sends the secret key K to the receiver by a secret channel. Since K is the secret key to decrypt the cipher image, we must send it to the legal receiver in secret. In general, there are two methods that can be used to distribute the secret key K. one is by a secure channel. The other is based on the computational difficulty of computing discrete logarithms (Kotulski and Szczepanski, 1997).

Kang *et al.* (2013) noted that compression of encrypted data draws much attention in recent years due to the security concerns in a serviceoriented environment such as cloud computing. The researchers proposed a scalable lossy compression scheme for images having their pixel value encrypted with a standard stream cipher. The encrypted data are simply compressed by transmitting a uniformly sub sampled portion of the encrypted data and some bit planes of

another uniformly sub sampled portion of the encrypted data. At the receiver side, a decoder performs content-adaptive interpolation based on the decrypted partial information, where the received bit plane information serves as the side information that reflects the image edge information, making the image reconstruction more precise. When more bit planes are transmitted, higher quality of the decompressed image can be achieved. The experimental results show that the proposed scheme achieves much better performance than the existing lossy compression scheme for pixel-value encrypted images and also similar performance as the state of-the art lossy compression for pixel permutation based encrypted images. In addition, the proposed scheme had the following advantages: at the decoder side, no computationally intensive iteration and no additional public orthogonal matrix were needed. It works well for both smooth and textured-rich images.

The One-dimensional Logistic Map

Chaotic dynamics was made popular by computer experiments of Robert May and Mitchell Feigenbaum on a one-dimensional map known as the logistic map. The remarkable feature of the logistic map is in the simplicity of its form and the complexity of its dynamics. It is the simplest model that shows chaos (Biswas, 2013). One of the most studied examples of a one-dimensional system capable of various dynamical regions including chaos is the one-dimensional logistic map. It is a representation of an idealized population growth model and is defined by the equation;

$$x_{n+1} = f_{\mu}(x_n) = \mu x_n(1 - x_n) \qquad (1)$$

The parameter μ lies in the interval [0,4]. The graph of f_{μ} is given in Figure 1 for $\mu=2$. Note that the maximum value of f_{μ} is always $\mu/4$. This can be computed as follows:

$f'_{\mu} = \mu(1 - 2x)$

Setting $f^1_{\mu} = 0,\ x = \frac{1}{2}$ is the maximum point since $f''_{\mu} = -2\mu < 0$.

The maximum value of f_{μ} is then;

$f_{\mu}(½) = \mu(½)(1 - ½) = \frac{\mu}{4}$.

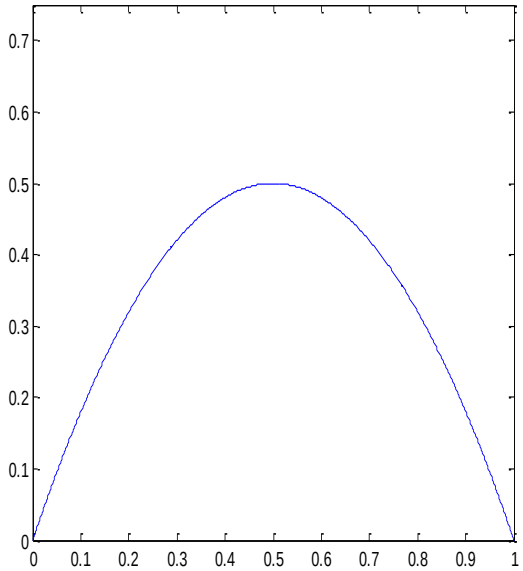


Figure 1: The logistic map function for $\mu=2$.

To find the points of period one (the fixed points), it is necessary to solve the equation given by;

$f_\mu(x) = \mu x(1 - x) = x$

which gives the points that satisfy $x_{n+1} = x_n$, for all n (Lynch, 2004).

There are two solutions $x_{1,1} = 0$ and $x_{1,2} = 1 - \frac{1}{\mu}$. The stability of the critical points may be determined by the following theorem;

Theorem 1

Suppose that the map $f_\mu(x)$ has a fixed point at x^*, then the fixed point is stable if

$\left| f_\mu^1(x^*) \right| < 1$ (a sink) and it is unstable (a source) if $\left| f_\mu^1(x^*) \right| > 1$.

For the logistic map,

$\left| f_\mu^1(0) \right| = \mu$ and $\left| f_\mu^1(x_{1,2}) \right| = 2 - \mu$.

For $0 \leq \mu < 1$, $x_{1,1}$ is stable while $x_{1,2}$ is unstable. For $\mu > 1$, $x_{1,1}$ is unstable while $x_{1,2}$ becomes stable for $1 < \mu < 3$ since $\left| 2 - \mu \right| < 1$ which also becomes unstable for $\mu > 3$ and period two sink takes its place. To find points of period two, it is necessary to solve the equation given by;

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

which gives the points that satisfy the condition $x_{n+2} = x_n$ for all *n*.

Two solutions of this equation are known, $x_{1,1}$ and $x_{1,2}$ since points of period one repeat on every second iterate. Therefore, to find other periodic points of equation (3.2), we reduce equation (3.2) from quartic to quadratic as follows;

$$b(x) = \frac{f^2(x) - x}{f(x) - x} = \mu^2 x^2 - (\mu^2 - \mu)x + \mu + 1$$

$$= 0 \qquad (3)$$

Equation (3) has roots at;

$$x_{2,1} = \frac{\mu + 1 + \sqrt{(\mu - 3)(\mu + 1)}}{2\mu} \text{ and}$$

$$x_{2,2} = \frac{\mu + 1 - \sqrt{(\mu - 3)(\mu + 1)}}{2\mu}.$$

Thus, there are two points of period two when $\mu > 3$. Let $b_1 = \mu = 3$ correspond to the first bifurcation point for the logistic map. Now;

$$\frac{\mathrm{d}}{\mathrm{d}x} f_\mu^2(x) = -4\mu^3 x^3 + 6\mu^3 x^2 - 2(\mu^2 + \mu^3)x + \mu^2$$

Where $\left| \frac{\mathrm{d}}{\mathrm{d}x} f_\mu^2(x_{1,1}) \right| > 1$ and $\left| \frac{\mathrm{d}}{\mathrm{d}x} f_\mu^2(x_{1,2}) \right| > 1$ but, $\left| \frac{\mathrm{d}}{\mathrm{d}x} f_\mu^2(x_{2,1}) \right| < 1$ and $\left| \frac{\mathrm{d}}{\mathrm{d}x} f_\mu^2(x_{2,2}) \right| < 1$

Thus, the first two are repelling fixed points while the other two are period-two points which are attracting points for $|4 + 2\mu - \mu^2| < 1$. Every point is eventually attracted to this period-two points for $3 < \mu < 1 + \sqrt{6}$. Let $\mu = b = 1 + \sqrt{6}$. The value b corresponds to the second bifurcation point for the logistic map. When $\mu > 1 + \sqrt{6}$, $x_{2,1}$ and $x_{2,2}$

lose their stability and period four is created. We can see that as the parameter, μ, increases, the orbit splits in an ordered fashion, which represents a qualitative change in the dynamic's behaviour of the map. This "bifurcation "process of splitting into period-2^n (n = 0,1, 2…) continues and ends at about μ = 3.57 and is called period-doubling bifurcation. For values of $\mu > 3.57$, the system becomes chaotic and up to $\mu = 4.00$, and $\mu > 4.00$, all the orbits escape to infinity.

Figure 2 shows the bifurcation diagram of the logistic map given by equation (3.1) as the parameter μ ϵ [0,4] is varied.

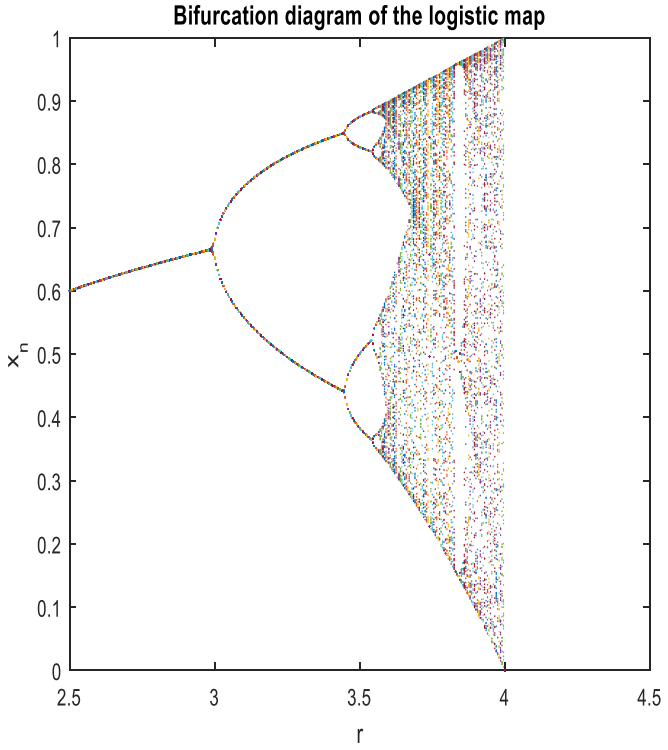


Figure 2: Bifurcation Diagram of the Logistic Map for μ ϵ [0,4]

A chaotic orbit is one that forever continues to experience the unstable behaviour that an orbit exhibits near a source, but that is not itself fixed or periodic. It never manages to find a sink to be attracted to. At any point of such an orbit, there are points arbitrary near that will move away from the point during further iteration. This sustained irregularity is quantified by Lyapunov number and Lyapunov exponent that is often used to determine whether or not a system is chaotic. The term Lyapunov number is introduced to quantify the average per-step divergence rate of nearby points along the orbit and Lyapunov exponent to be the natural logarithm of the Lyapunov number (Alligood,1996).

Lyapunov Exponents

According to Lynch (2004), another method often used to determine whether or not a system is chaotic is the Lyapunov exponent. The formular below may be applied to compute the Lyapunov exponent for iterates in the logistic map. It gives an indicator as to whether two orbits starting close together diverge or converge.

Definition: The Lyapunov exponent L computed using the derivative method is defined by;

$$L = \frac{1}{n}[ln \mid f'_{\mu}(x_1) \mid + ln \mid f'_{\mu}(x_2) \mid + \cdots + ln \mid f'_{\mu}(x_n) \mid]$$

where $x_1, x_2, \ldots, x_n$ are successive iterates.

The Lyapunov exponent may be computed for a sample of points near the attractor to obtain an average Lyapunov exponent.

Theorem 2 (Lynch, 2004)

If, at least, one of the Lyapunov exponents is positive, then the system is chaotic; if the average Lyapunov is negative, then the orbit is periodic, and when the average Lyapunov exponent is zero, then a bifurcation occurs.

Weaknesses of the One-dimensional Logistic Map

The one dimensional chaotic system's drawbacks include small key space and weak security. Logistic maps are faced with the problem of lack of robustness of their encryptions because of round off errors in real number quantization. This may lead to nonreversible functions for encryption and this makes decryption process impossible. The third defect reveals a high risk that initial values and parameters used in a chaotic system might be fully analyzed using existing tools and methods after a long term observation.

The Modified One-Dimensional Logistic Map

The proposed modified one-dimensional logistic map is defined by

$$x_{n+1} = f(x_n) = \mu x_n(1 - x_n)\cosh(x),$$

where $x_n \in [0,1]$ and where $\mu \in [0, 3.5]$ is the control parameter. Slight changes in the values of the parameter "μ'' of the map can cause the iterated map to change from stable and predictable behaviour to unpredictable behaviour which is called chaos. Figure 3 shows the bifurcation diagram of the modified logistic map. From the figure, we observed that when the control parameter $\mu < 1$, all the points are plotted at zero, i.e., zero is the one-point attractor for $\mu < 1$. The figure also shows that when $1 < \mu < 2.9$, we still have a one-point attractor, but the "attracted" value of x increases as μ increases, at least to 2.76. Bifurcations occur first at $\mu = 2.76$, then $\mu = 3.1$ and $\mu = 3.2$ (approximately) until just beyond $\mu = 3.35$ where the system becomes chaotic up to $\mu = 3.5$ which can generate a chaotic sequence in the region (0,1). The orbits escape to infinity for $\mu > 3.5$.

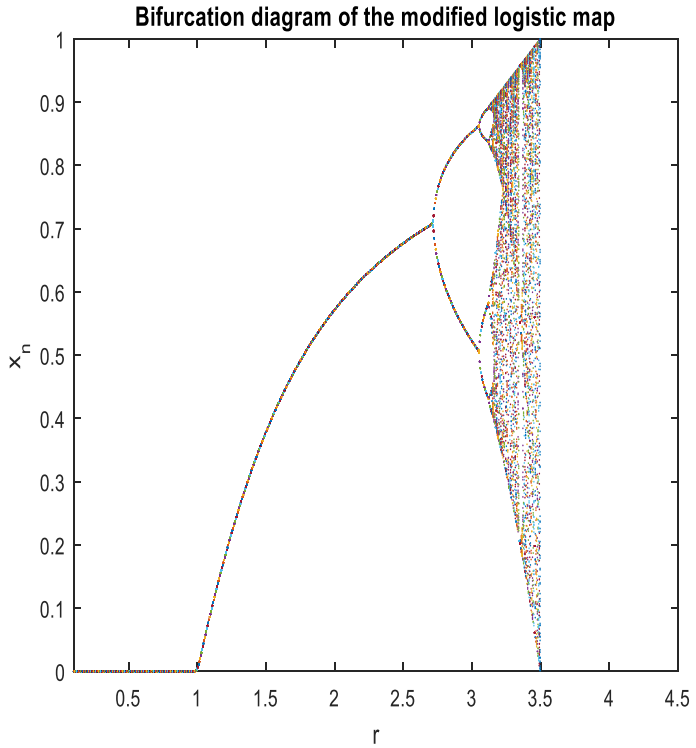


Figure 3: Bifurcation Diagram of the Modified One-Dimensional Logistic Map for $\mu \in [0, 3.5]$

Fixed Points and Periodic Points of the Modified Logistic Map.

To find the fixed points of the points of period one, the equation

$f_\mu(x) = \mu x(1 - x)\cosh(x) = x$ is solved so that

$\mu x(1 - x)\cosh(x) - x = 0$

$x[\mu(1 - x)\cosh(x) - 1] = 0$

The fixed points are $x_{1,1} = 0$

and the root of $\mu(1 - x)\cosh(x) - 1 = 0$ (4.1)

or

$\mu\cosh(x) - \mu x\cosh(x) = 1$

This can be expressed as $\mu(\frac{e^x + e^{-x}}{2}) - \mu x[\frac{e^x + e^{-x}}{2}] = 1$

or $\mu x e^x + \mu x e^{-x} - \mu e^x - \mu e^{-x} + 2 = 0$

Multiplying through by e^xgives;

$\mu x e^{2x} + \mu x - \mu e^{2x} - \mu + 2e^x = 0$

The other fixed point can be found using Newton's iteration as follows;

$$t(x) = \mu x e^{2x} + \mu x - \mu e^{2x} - \mu + 2e^x$$

$$t'(x) = -\mu e^{2x} + 2\mu x e^{2x} + \mu + 2e^x$$

and the iteration is given by;

$$x_{k+1} = x_k - \frac{t(x_k)}{t'(x_k)}$$

These can be obtained numerically using a simple code in MATLAB found in the Appendix. Some results are given below.

To investigate the stability of the fixed points, note that

$f_\mu(x) = \mu x(1 - x)\cosh(x)$

differentiating with respect to x

$f_\mu^1(x) = \mu(1 - x)\cosh(x) - \mu x\cosh(x) + \mu x(1 - x)\sinh(x)$

$= -\mu[-\cosh(x) + 2x\cosh(x) - x\sinh(x) + x^2\sinh(x)]$,

Now $f_\mu^1(0) = \mu$. From theorem 1, the fixed point $x_{1,1}$ is stable for $0 < \mu < 1$ and unstable if $\mu > 1$.

The other fixed points are stable when

$$\left| \mu[-\cosh(x) + 2x\cosh(x) - x\sinh(x) + x^2\sinh(x)] \right| < 1.$$

For points of period two, the equation

$f_\mu^2(x) = x \quad \rightarrow \quad f_\mu(f_\mu(x)) = x$ needs to be solved

$f_\mu[\mu x(1 - x)\cosh(x)] = x$

or

$$\mu[\mu x(1 - x)\cosh(x)][1 - \mu x(1 - x)\cosh(x)][\cosh(\mu x(1 - x)\cosh(x))] = x$$

$$\mu^2 x(1 - x)(1 - \mu x\cosh(x) + \mu x^2\cosh(x))\cosh(\mu x(1 - x)\cosh(x)) = x$$

solving gives the points of period two of the modified map. This a complicated nonlinear equation but the points can be estimated using Newton's method or by using a computer algebra software.

Image Encryption

Encryption of sensitive images in this modern age of technology has become necessary for ensuring that such images sent via the insecure public network called the internet are protected from attacks. To this end, various image encryption algorithms have been proposed by researchers. These algorithms are designed either based on chaotic properties of some dynamical systems and

are referred to as chaos-based encryption schemes or are designed on the properties of good mixing and computational complexity, and are called non-chaos-based encryption schemes (Fredrich, 1997; Kester and Koumadi, 2012; Goldriech, 2004).

Image Encryption Algorithm Using the Modified One-Dimensional Logistic Map

In this section, we present the detail algorithm for encryption/decryption of gray scale images using the modified one – dimensional logistic map.

Encryption algorithm

- Read the original image I,
- Obtain the image dimension *a* and *b*,
- Compute the number of pixels in I, N,
- Read the parameters value for the x_1, and μ,
- Evaluate the logistic map up to N-1 times to generate vector X,
- Add confusion to the vector X with mod function,
- Convert the vector X to integer,
- Perform the encryption using the bit XOR operation,
- Save the encrypted image in the file named I2.
- Display the encrypted image from file I2.

Decryption algorithm

- Read the encrypted image file I2,
- Obtain the image dimension *a* and *b*,
- Compute number of pixels in I2, N,
- Enter your parameter value for y_1 and μ,
- Evaluate the logistic map up to N -1 times to generate vector Y,
- Confuse the vector Y with mod function,
- Convert vector Y to integer,
- Perform the decryption process using bit XOR operation,
- Save the decrypted image as I3,
- Display the decrypted image I3.

Performance Analysis of the Proposed Cryptosystems

With the application of an encryption algorithm to an image, it is expected that its pixel values change when compared with the original image. A good encryption algorithm must make these changes in an irregular manner and maximize the difference in pixel values between the original and the encrypted images. Also, to obtain a good encrypted image, it must be composed of totally random patterns that do not reveal any of the features of the original image. That is, an encrypted image has to be independent of the original image and therefore, it should have a low correlation with the original image.

Two families of encryption metrics are available for qualitative evaluation of encryption algorithms. The first family constitutes the statistical analysis which evaluates the ability of an encryption algorithm to substitute the original image with an uncorrelated encrypted image i.e, to measure how good the encryption algorithm can stand against the statistical attack. In the family, we considered only two metrics: The Correlation Coefficient Analysis and the Histogram Uniformity Analysis. The second family called the sensitivity analysis also called the differential analysis evaluates the diffusion characteristics of the encryption algorithm which is an important parameter that must be measured to judge the encryption algorithm randomization, if an encryption algorithm has a good diffusion characteristic, the relation between the encrypted image and the original image is too complex, and it cannot be predicted easily. In the family, we considered two metrics also: The Number of Pixel Change Rate (NPCR), and the Unified Average Changing Intensity (UACI) (Abd El-Samie et al., 2014; Stoyanov and Korodv, 2014; Ramadan et al., 2016).

Correlation coefficient analysis

A useful metric to assess the encryption quality of any image encryption algorithm is the correlation coefficient between adjacent pixels of the cipher-image. In our proposed encryption algorithm, we analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in the cipher-image, we also obtained the same correlation

coefficient in the plain-image for comparison purpose, this metric is calculated as follows:

$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$

Where *x* and *y* are the values of two adjacent pixels in the cipher-image. In numerical computation, the following discrete formulas can be used:

$E(x) = \frac{1}{L}\sum_{l=1}^{L} x_l$, $D(x) = \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))^2$, and

$Cov(x,y) = \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))(y_l - E(y))$

Where L is the number of pixels involved in the calculations, the closer the value of r_{xy} to zero, the better the quality of the encryption algorithm will be (Sathishkumar et al., 2011; Abugharsa et al., 2011; Ye, 2013, Abd El-Samie et al., 2014).

Histogram Uniformity Analysis

A histogram uses a bar graph to profile the occurrence of each gray level of the image, the horizontal axis represents the gray-level value, it begins at zero and goes to the number of gray levels, each vertical bar represents the number of occurrences of the corresponding gray level in the image. For image encryption algorithm to be considered worthy of use, the histogram of the encrypted image should satisfy these two properties (Abd El-Samie et al., 2014):

i) It must be totally different from the histogram of the original image.

ii) It must have a uniform distribution, which means that the probability of occurrence of any gray scale value (monochrome) is the same.

Sensitivity Analysis (Differential Analysis)

In general, an encrypted image must be sensitive to small changes in the original image. If one minor change in the plain-image will cause a significant change in the cipher-image, then the encryption scheme will resist the differential attack efficiently. To test the influence of only one pixel, change in the plain-image over the whole cipher-image, we used two common measures: The Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). The NPCR measures the percentage of different pixels` number between the two cipher-image whose plain-image only have one pixel difference, whereas, the UACI measures the average intensity of differences between the two cipher-images, they indicate the sensitivity of the cipher-image to the minor change of plain-image. The formular for evaluating NPCR and UACI are as follows:

$NPCR = \frac{\sum_{i,j} D(i,j)}{W\ X\ H}$ x 100% and UACI = $\frac{1}{W\ X\ H}[\sum_{i,j}\frac{C_1(i,j) - C_2(i,j)}{255}]$ x 100%

Where C_1 and C_2 denote the two ciphered image whose corresponding plain-image have only one pixel difference, the $C_1(i,j)$ and $C_2(i,j)$ represent the gray scale value of the pixels at grid (i,j) in the C_1 and C_2 respectively, the D(i,j) is a binary matrix with the same size as the image C_1 and C_2 whose entries is determined from $C_1(i,j)$ and $C_2(I,j)$ by the following: if $C_1(i,j) = C_2(i,j)$, then D(i,j)=0, otherwise, D(i,j)=1. The W and H are the width and height of the image, the higher the values of NPCR and UACI, the stronger the encryption algorithm is to resist a differential attack (Borujeni and Eshghi, 2009; Abugharsa et al., 2011; Wu et al., 2011; Ye, 2013; Stoyanov and Kordov, 2014; Abd El-Samie et al., 2014; Ramandan et al., 2016).

RESULTS AND DISCUSSION

This chapter consists of the results obtained in this work. The results were obtained using MATLAB codes which are presented in the appendix.

4.1 Iterates of the Modified Logistic Map

The orbits of the modified logistic map are plotted in Figure 4 – 6 where $x_0 = 0.2$ and for (i), $\mu = 1.4$, (ii) $\mu = 2.8$, (iii) $\mu = 3.15$, (iv) $\mu = 3.3$, (v) $\mu = 3.45$. The function, μ, varies between 1 to 3.5, not 1 to 3.5 since the end points are not included. It was observed that the function $f_\mu(x) = \mu x(1 -$

$x)\cosh(x)$ exhibits extraordinary variety of behaviours as μ varies from 1 to 3.5. This reveals that simple equation can lead to extremely complex seemingly random behaviour.

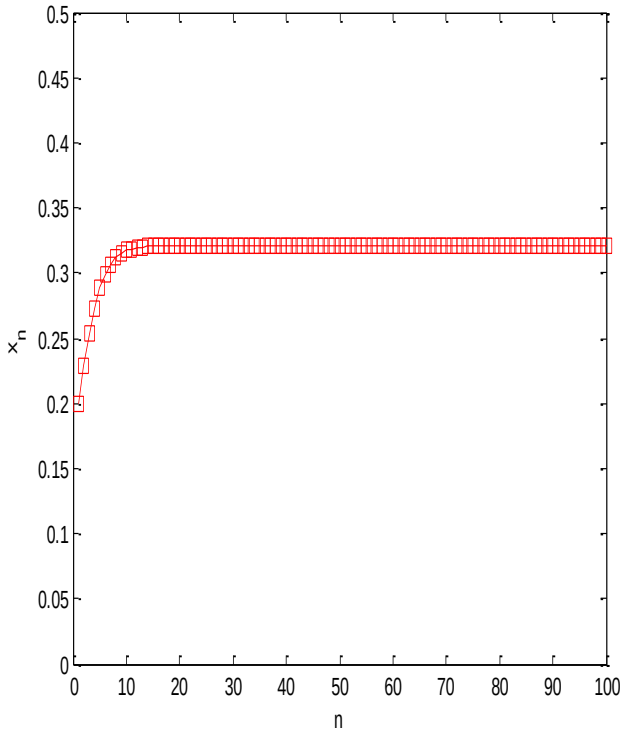


Figure 4: Orbits of the modified logistic map at μ = 1.4 and x_0=0.2 showing convergence to a fixed point

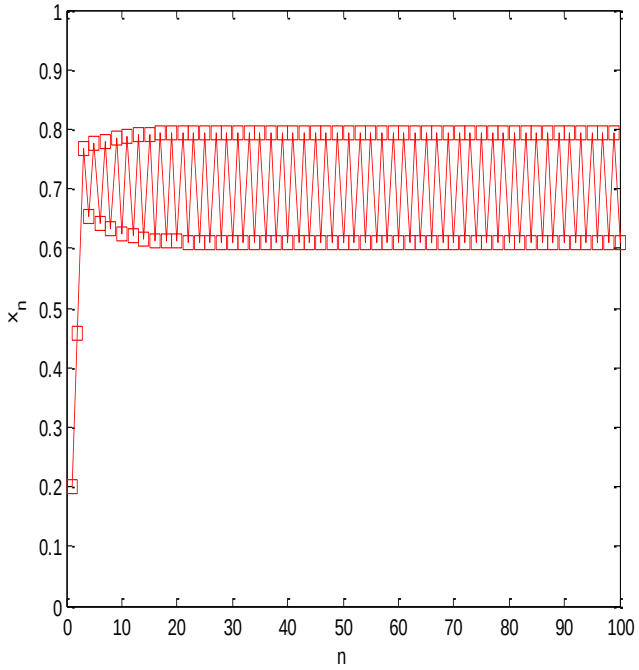


Figure 5: Orbits for the modified logistic map

at $\mu = 2.8$ and $x_0=0.2$ showing periodicity of two

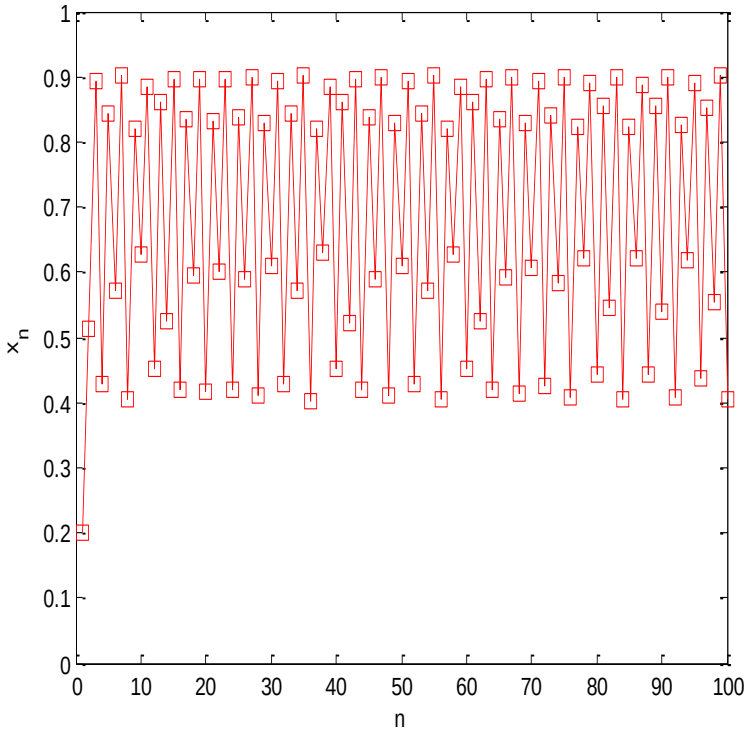


Figure 6: Orbits for the modified logistic map at $\mu = 3.15$ and $x_0=0.2$ showing periodicity of four

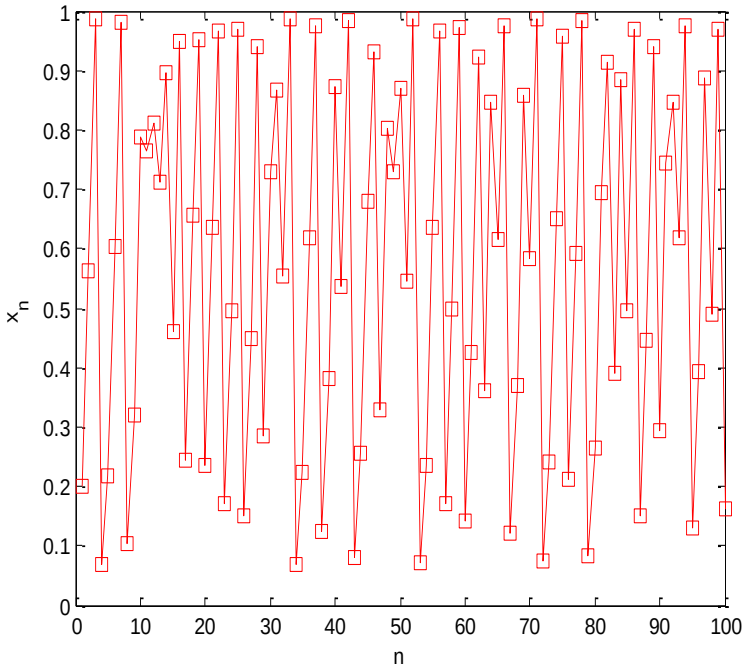


Figure 7: Orbits for the modified logistic map at $\mu = 3.45$ and $x_0=0.2$ showing chaos

These results follow the bifurcation diagram in Figure 3 which shows a period doubling bifurcation. As μ increases beyond μ = 2.76, points of period one (fixed point) becomes period two: at μ = 3.1, points of period two become period four and so on. The sequence of period doubling ends around μ = 3.35 where the system becomes chaotic. In Figure 4, the orbit with μ = 1.4 tends to a point 0.3210 of period 1 while in Figure 5, the orbit with μ = 2.8, displays a period two behaviour oscillating between 0.6104 and 0.7938. In Figure 6, the orbit for μ = 3.15 is a period four sequence while at μ = 3.45 in Figure 7, the orbit displays chaotic behaviour.

It is obvious that the modified logistic map displays a rich variety of dynamics for different values of μ.

Encryption of Digital Images Using the Modified Logistic Map

In this section, we will use the encryption algorithm based on the modified logistic map to encrypt two standard test images.

Figure 8 displays the original image, the cipher image and the decrypted images for lena-gray-256.tif which is a 256 x 256 pixels image. Figure 9 shows the various images for mandril-gray.tif.

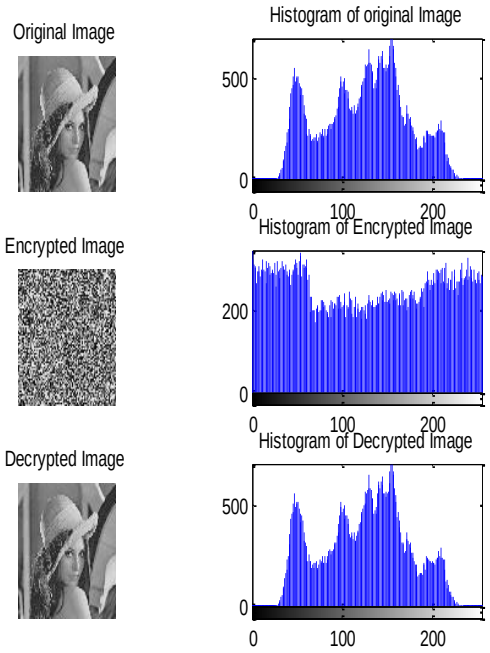


Figure 8: Original, encrypted and decrypted lena image with their histograms using the modified logistic map image encryption algorithm.

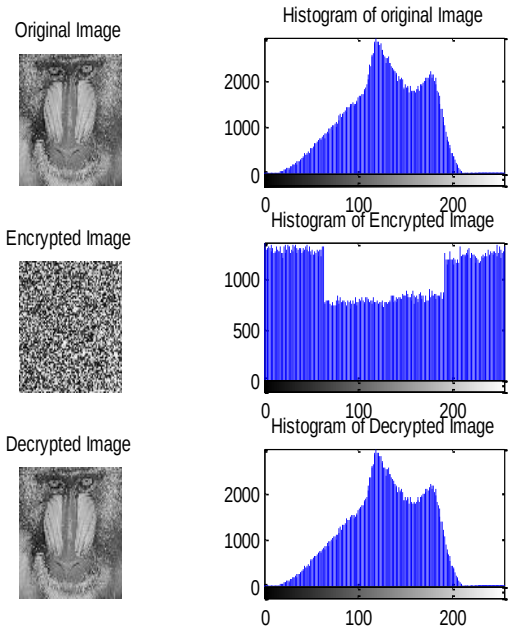


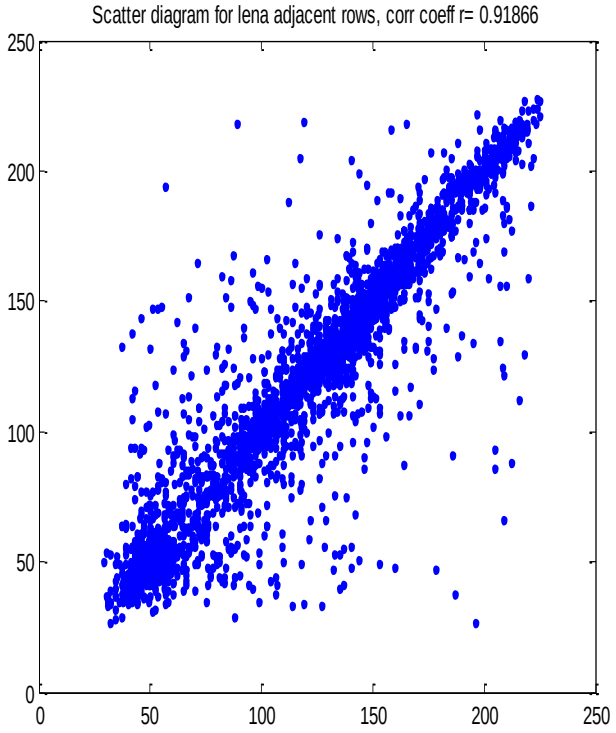
Figure 9: Original, encrypted and decrypted mandril_gray image with their histograms using the modified logistic map.

The image histogram is a graphical representation that shows the distribution of pixel intensity values within the image. Each pixel has a brightness values between 0 (black) and 255 (white), with varying shades of gray in between. It is a bar graph where the x-axis represents all possible intensity values (0 to 255). The y-axis shows the frequency (number of pixels) that have each intensity.

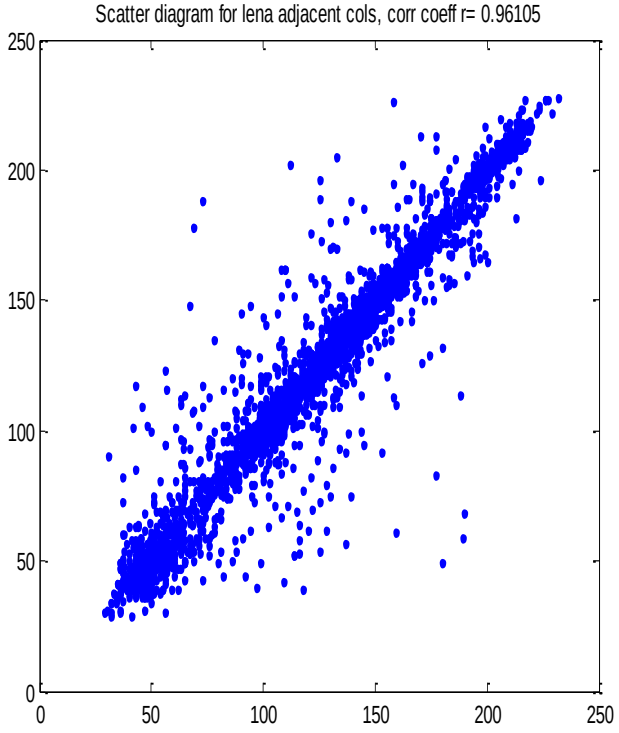
It is observed that the proposed algorithms performed well on both images and the histogram of the decrypted image is almost identical with the histogram of the original image. The histogram of the encrypted image is significantly different from the image of the original image. In addtion, the histogram of the encrypted image is generally flat as required of a good encryption algorithm.

Performance Analysis of Encryption Schemes

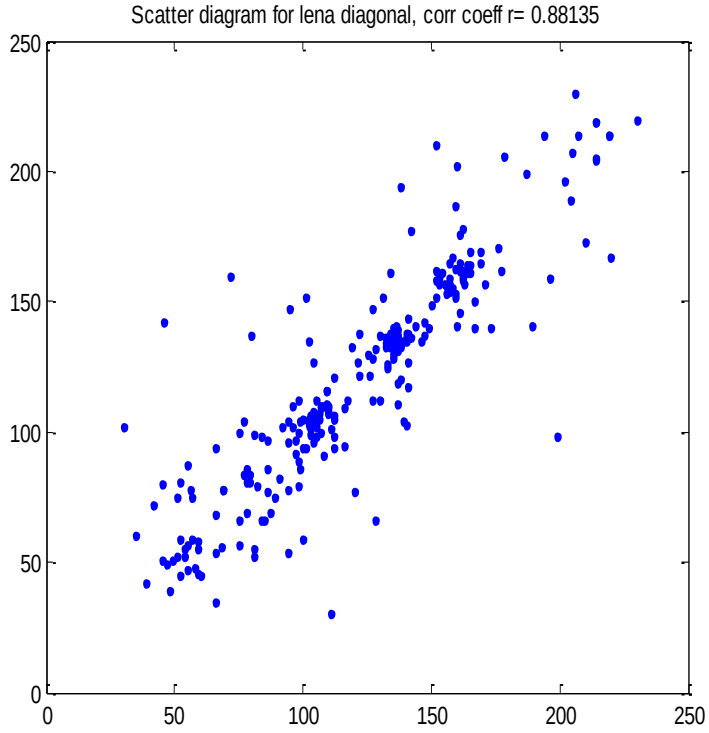
In this section, the scatter diagram for the various images are presented.



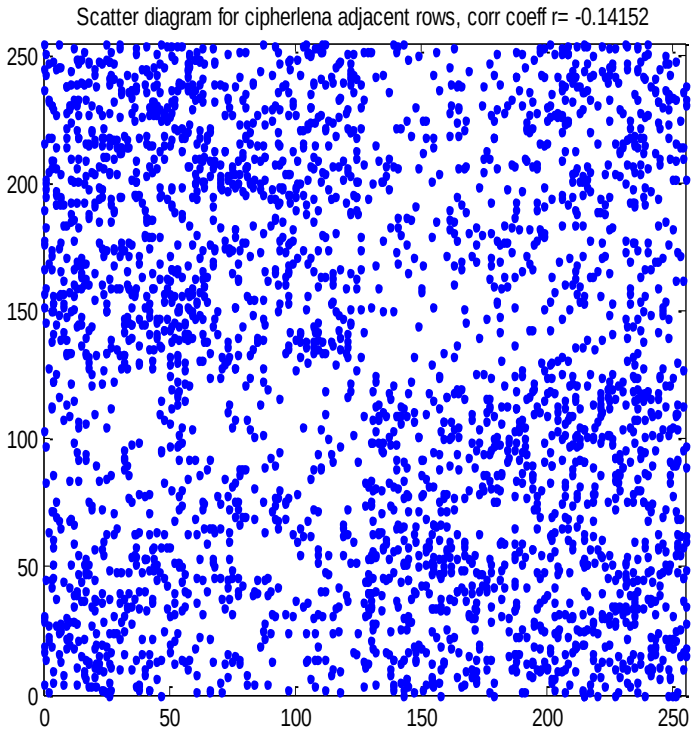
(a)



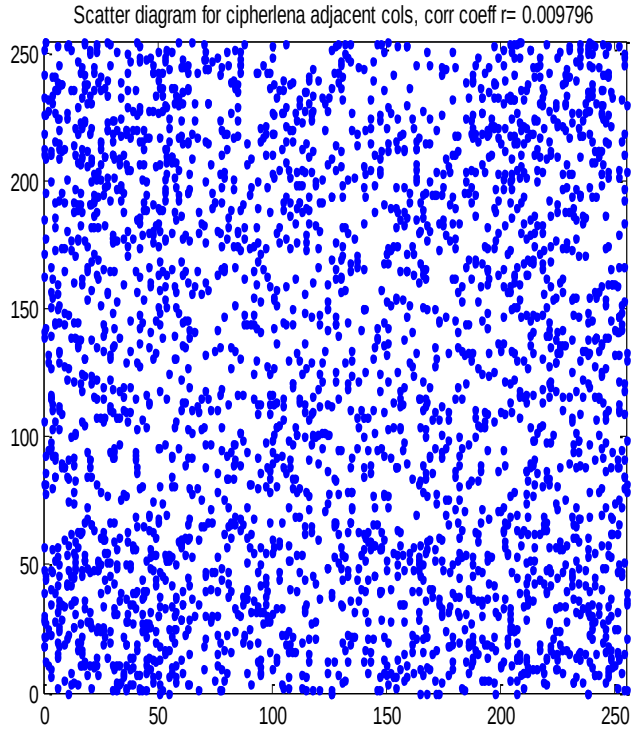
(b)



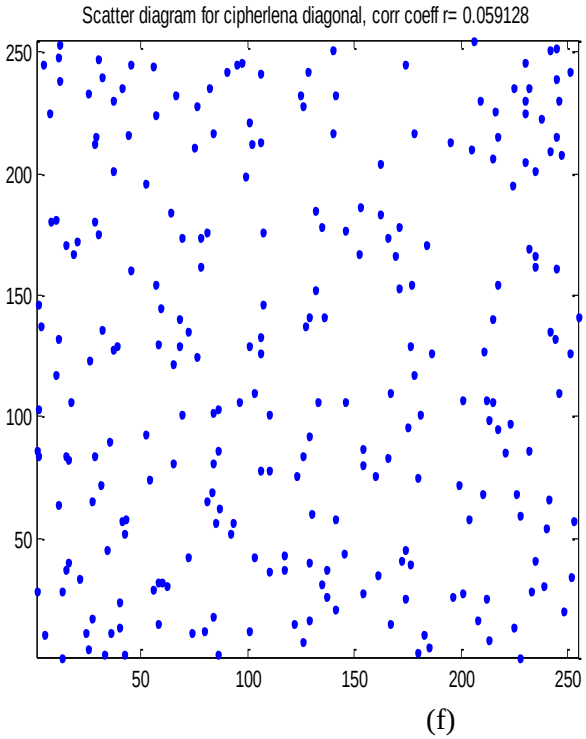
Cipher Lena



(d)



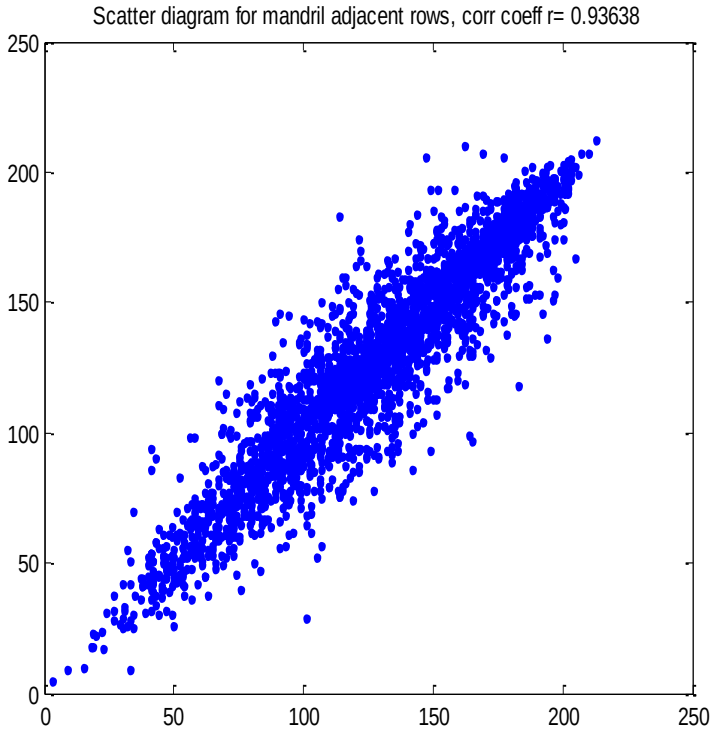
(e)

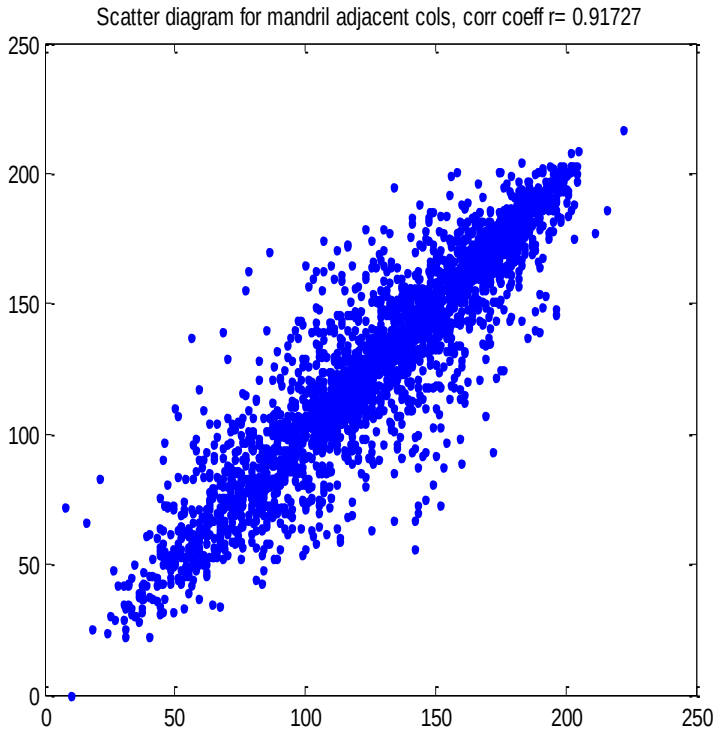


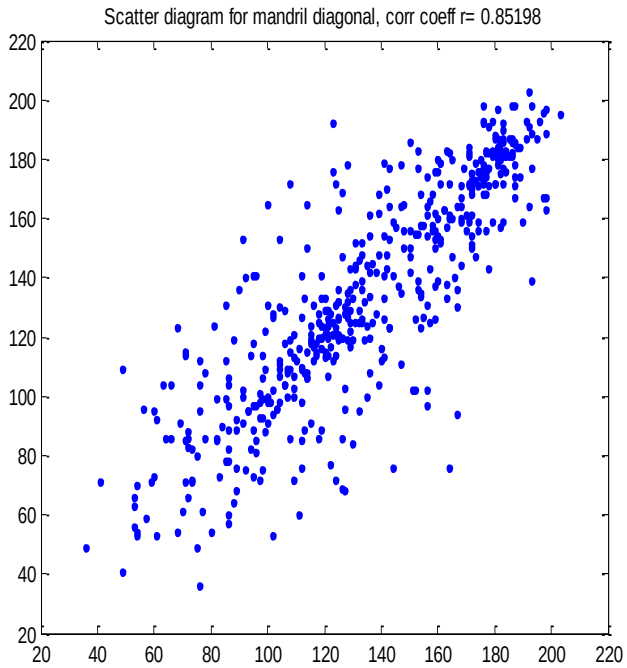
(f)

Figure 10: Scatter Diagram and correlation coefficient between adjacent pixels of the plain and cipher images of lena for the rows, columns and diagonal.

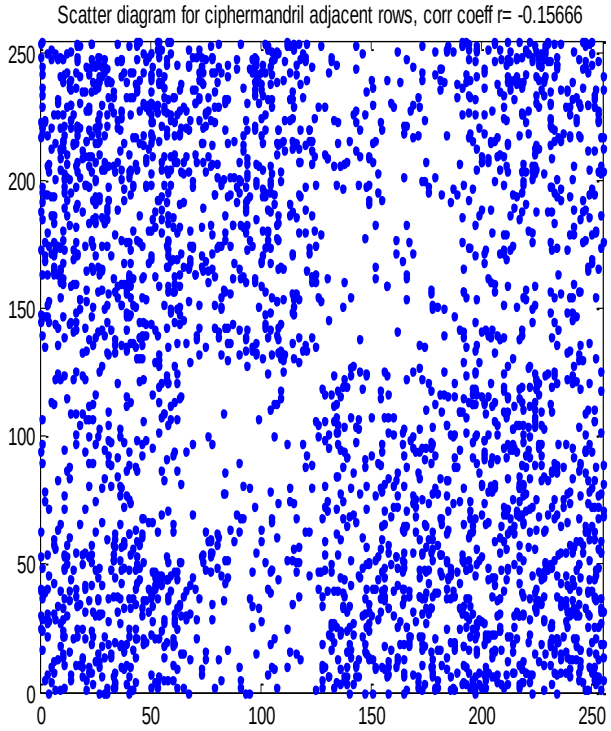
Mandril


Scatter diagram for mandril adjacent rows, corr coeff r= 0.93638
250
200
150
100
50
0
0
50
100
150
200
250


Scatter diagram for mandril adjacent cols, corr coeff r= 0.91727
250
200
150
100
50
0
0
50
100
150
200
250



Mandril Cipher



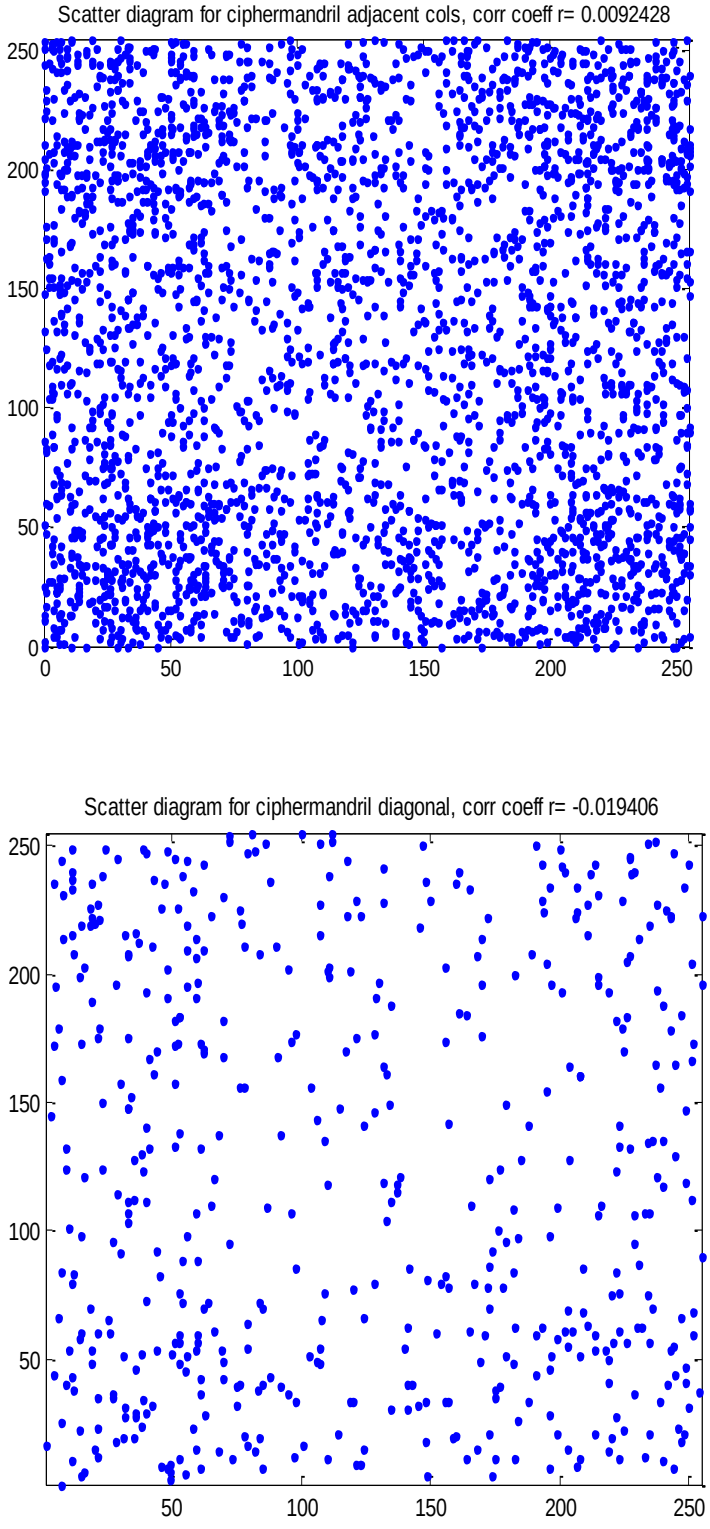


Figure 11: Scatter Diagram and correlation coefficient between adjacent pixels of the plain and cipher images of mandril for the rows, columns and diagonal.

Table 1: Correlation coefficient of plain and cipher images for the rows, columns and diagonal for lena and mandril images

	Image			
	Lena		Mandril	
	Plain	Cipher	Plain	Cipher
Row	0.919	-0.142	0.936	-0.157
Column	0.961	0.010	0.917	0.010
Diagonal	0.881	0.059	0.852	-0.019

A scatter diagram of neighbouring pixels shows a relationship between the intensity of adjacent pixels in an image. It usually plots the intensity of one pixel on the x-axis and its neighbouring pixel on the y-axis. This was done for 3000 random pixel pairs across the image for the rows (horizontal direction) and columns (vertical direction) and 360 pairs along the main diagonal.

In a good encryption algorithm, points in the scatter diagram of the original image form a dense cluster along the diagonal because natural images have high correlation between neighbouring pixels. However, for the encrypted image, points in the scatter plot should be scattered randomly with no visible structure or diagonal line.

The correlation coefficient quantifies the linear relationship between the intensity values of the neighbouring pixels as illustrated in the scatter diagram.

Figures 10 and 11 show the results of the correlation coefficient analysis (scatter diagram and correlation coefficients) of the modified logistic map on the lena and mandril images. It shows both the scatter diagrams and the correlation coefficients. A summary of the correlation coefficients is provided in Table 1. The plain images have high correlation coefficients in all three directions indication a very strong correlation as expected in natural images. The scatter diagrams are also heavily clustered along the diagonal line. The correlation coefficients for the cipherimages on the other hand are low in all three directions. The points scatter diagrams for the cipher image are scattered randomly with no visible patterns. This demonstrates the effectiveness of the encryption algorithm.

Lyapunov Exponents

The Lyapunov component L can be computed using the derivative method

$f_\mu(x) = \mu x(1 - x)\cosh(x)$

$f_\mu^1(x) = -\mu[-\cosh(x) + 2x\cosh(x) - x\sinh(x) + x^2\sinh(x)]$.

The Lyapunov exponent is therefore

$$L = \frac{1}{n}\sum_i ln\left|\mu[-\cosh(x_i) + 2x_i\cosh(x_i) - x_i\sinh(x_i) + x_i 2\sinh(x_i)]\right|$$

The Lyapunov exponent will be computed for a sample of points near the attractor to obtain an average Lyapunov exponent.

Table 2: Average Lyapunov exponent

M	0.5	1	2.2	2.72	3.05	3.2	3.4	3.5
Average L	-0.6932	-0.0034	-1.2198	-0.0034	-0.0711	0.2463	0.5048	Inf.

The Lyapunov exponents in Table 1 are computed to four decimal places using the first derivative method for the modified logistic map. A total of 50,000 iterates were used in each case and implemented in MATLAB.

Using Theorem 2, it is observed that the system is chaotic at 3.2 and 3.4, periodic at 2.2 while a bifurcation occurs at 1 and near 2.72 and 3.05. This agrees with the bifurcation diagram.

CONCLUSION

This paper has presented the development and analysis of a modified one-dimensional logistic map, with particular emphasis on its dynamical properties and application to image encryption. The modification introduced to the classic logistic map through the incorporation of the hyperbolic cosine function cosh(x) significantly enhanced the complexity and versatility of the map, resulting in a broader range of dynamic behaviours, including chaos, which was confirmed through bifurcation analysis and Lyapunov exponent calculations.

The theoretical analysis showed that the modified map retained essential properties such as fixed points, periodicity, bifurcation, and chaos, but with different threshold values for control parameters compared to the classical logistic map. These changes made the map more suitable for cryptographic applications due to its higher sensitivity to initial conditions and parameters.

The proposed image encryption algorithm based on this modified map was implemented and tested on standard grayscale images. The performance evaluation using correlation coefficient analysis, histogram uniformity, confirmed that the encryption scheme successfully obscured the original image features and introduced strong diffusion and confusion properties, both of which are essential for resisting statistical and differential attacks.

In conclusion, the modified logistic map developed in this study has demonstrated significant potential in the field of chaos-based cryptography and could serve as a foundation for secure and efficient encryption systems, particularly in image protection.

REFERENCES

Abd El-Latif, A. A., Zhang, T., Wang, N., Song, X. and Niu, X. (2012). Digital Image Encryption Scheme Based on Multiple Chaotic Systems, Sensing and Imaging. *International Journal on Continuing Subsurface Sensing Technologies and Applications*, 56(2): 67-68

Abd El-Samie, E. F., Ahmed, H. E. H., Elashry, F. I, Shahieen, H. M., Faragallah, S. O., El-Rabaie, M. E. and Alshebeili, A. S. (2014). Image Encryption-A Communication Perspective. 1st Edition. London: CRC Press, pp. 1-86

Abraham, L. and Daniel, N. (2013). Secure Image Encryption Algorithms: A Review. *International Journal of Scientific and Technology Research*, 2(4): 186 -189

Abugharsa, A. B., HassanBasari, A. S. B. and Almangush, H. (2011). A New Image Encryption Approach Using Bloc-Based on Shifted Algorithm. *International Journal of Computer Science and Network Security*, 11(12):123-130.

Alligood, K. T., Sauer, T. D. and Yorke, J. A. (1996). CHAOS- *An Introduction to Dynamical Systems*. New Yorke, USA: Springer-Verlag Inc., 553 pp.

Anju, S., Babita, G., Reena, M. and Aggarwal A. (2013). An Approach to Improve Data Security Using Encryption and Decryption Technique. *International Journal of Information and Computation Technology*, 3(3):125-130.

Biswas, R. H. (2013). One-Dimensional Chaotic Dynamical Systems. *Journal of Pure and Applied Mathematics: Advances and Applications*, 10(1):69-101.

Boriga, E. R., Dascalescu, A. C. and Diaconu, A. (2014). A New One-Dimensional Chaotic Map and its use in a Novel Real-Time Image Encryption Scheme. *Advances in Multimedia*, 2(1):1-15.

Cao et al. (2024). Complex hidden dynamics in a memristive map with delta connection and its application in image encryption.

Cao, Y. (2013). A New Hybrid Chaotic Map and Its Application on Image Encryption and

Hiding. *Mathematical Problems in Engineering*, 2(1):1-15.

Danca, M. F. and Chen, G. (2004). Bifurcation and Chaos in a Complex Model of Dissipative Medium. *International Journal of Bifurcation and Chaos*, 14(1):3409-3447.

Denning, D. E (1982). *Cryptography and Data Security*. USA: Addison-Wesley Publishing Company Inc., pp. 1-116.

Dinu and Frunzete (2025). Image Encryption Using Chaotic Maps.

Frdrich, J. (1997). Image Encryption Based on Chaotic Maps. *Proceedings of IEEE International Conference Systems, Man and Cybernetics*, 2(2):1105-1110.

Goldreich, O. (2004). Foundation of Cryptography Basic Techniques. 2nd Edition. UK: Cambridge University Press, pp. 1-63.

Gonzalez, R. C. and Woods, R. E. (2002). Digital Image Processing. 2nd Edition. USA: Prentice Hall, pp. 1-30.

Gonzalez, R. C. and Woods, R. E. and Eddins, S. L. (2009). *Digital Image Processing Using MATLAB*. 2nd Edition. USA: Gatesmark Publishing LLC. Pp. 1-85.

Hoffstein, J., Pipher, J. and Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. 1st Edition. New York. USA: Springer Science + Business Media, pp. 10-65.

Jain, M. K., Iyengar, S. R. K. and Jain, R. K. (2007). Numerical Methods for Scientific and Engineering Computation. 5th Edition. New Delhi-India: New Age International (p) Limited. pp. 403-484.

Jastrzebski, K. and Kotulski, Z. (2009). Improved Image Encryption Scheme Based on Chaotic Map Lattices. Engineering Transactions. 57(2): 69-84.

Kokarev, L., and Lian, S. (2011). *Chaos-Based Cryptography*: Theory, Algorithms and Applications. Berlin Heidelberg: Springer-Verlag, pp. 1-65.

Liang and Zhu (2023). A novel one-dimensional chaotic system for image encryption scheme based on random DNA coding.

Lynch, S. (2004). *Dynamical Systems with Applications Using MATLAB*. New Yorke. USA: Springer Science + Business Media, LLC., pp 35-68, & 271-294.

Mishra, M. and Mankar, V. H. (2011). Chaotic Encryption Scheme Using 1-D Chaotic Map. *International Journal of Communications, Network and System Sciences*, 4(10): 452-455.

Pareek, N. K., Patidar, V. and Sud, K. K. (2006). Image Encryption Using Chaotic Logistic Map. *Image and Vision Computing*, 24(2006): 926-734.

Prasad, M. and Sudha, K. L. (2011). Chaos Image Encryption Using Pixel Shuffling. *Computer Science and Information Technology*, 2(1): 169-179.

Sakthidasan@Sankaran, K. and Krishna, B. V. S. (2011). A New Chaotic Algorithm for Image Encryption and Decryption of Digital Colour Images. *International Journal of Information and Education Technology*, 1(2): 137-141.

Solomon, C and Breckon, T. (2011). *Fundamentals of Digital Image Processing*. UK: John Wiley and Sons Ltd., pp. 1-81.

Stallings, W. (2011). Cryptography and Network Security Principles and Practices. 5th Edition. USA: Pearson Education Inc., 567pp.

Trappe, W. and Washington, L. C. (2006). *Introduction to Cryptography with Coding Theory*. 2nd Edition. USA: Pearson Education Inc., pp. 21-65.

Wei Feng et al. (2024). Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption.

Wu, Y., Yang, G., Jin, H. and Nooman, J. P. (2012). Image Encryption Using the Two-Dimensional Logistic Chaotic Map. *Journal of Electronic Imaging*. 21(1): 1-29.

Yakubu, H. J. and Aboiyar, T. (2016). Comments on "Rivest-Shamir-Adleman (RSA) Image Encryption Algorithm". Nigerian Journal

of Pure and Applied Sciences, 8(1): 216-223.

Yang et al. (2022). Image encryption scheme based on mixed chaotic Bernoulli measurement matrix block compressive sensing.

Ye, R. (2013). A Highly Secure Image Encryption Scheme Using Compound Chaotic Maps. *Journal of Emerging Trends in Computing and Information Sciences*, 4(6): 532-544.

Yingfang Zhu and Erxi Zhu (2025). A multi-image encryption algorithm based on hybrid chaotic map and computer-generated holography