China Petroleum Processing and Petrochemical Technology

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

"A STUDY OF DESIGN AND ANALYSIS OF CHAOTIC MAP AND CHAOTIC KEY BASED ENCRYPTION ALGORITHMS FOR COLOR DIGITAL IMAGES"

Renuka Patel
Research Scholar, Computer Science Department, Madhyanchal Professional University, Ratibad, Bhopal (M.P.) India

Ankit Temurnikar
Guide, (Assistant Professor) Computer Science Department
Madhyanchal Professional University, Ratibad, Bhopal (M.P.) India

ABSTRACT: The enormous growth in communication networks and communication devices has created great potential for multimedia generation and transmission, especially in terms of images. Digital images are vulnerable to security threats, with security concerns looming large. Consequently, there is a need for security measures to be put in place, and a variety of encryption schemes have been proposed to address this challenge. Schemes formulated for textual data are not suited to images, owing to various inherent features as high pixel frequency, volume of data, and close correlation among pixels. As a solution, chaos-based cryptosystems have emerged as a field in cryptography and found to deal with images efficiently. A well-defined chaos based image cryptosystem is a combination of confusion and diffusion processes. In the confusion process, the pixel positions are changed and in the diffusion process, pixel values are changed.

In this paper, appropriate chaotic maps are identified for use in the confusion and the diffusion phases of image encryption. Techniques based on these chaotic maps are combined together to form desirable image cryptosystems. The objective of this work is to develop and implement a cryptosystem for images having unequal dimensions.The Arnold transform is the simplest and frequently-used confusion technique. The basis matrices of the Arnold transform are combined together with their mirrors to produce new enhanced transformation matrices. The enhanced Arnold transform (EAT) matrices can be used in the confusion phase of any image cryptosystem to mystify the relationship between the plain image and the scrambled image.

KEY WORDS: Engineering and technology computer science , computer science information system cryptosystem color images.

INTRODUCTION: 21st century is the century of innovation and technology. In its early years, we saw a rapid progress in every aspect of life. Social media and communication sector revolutionized in previous two decades. Internet has completely changed the way of communication and socializing with each other. In many of our daily use internet applications like Facebook, WhatsApp, Video conferencing, Skype etc., we have to deal with digital images. [12]Digital image communication is also used in some sensitive institutions like military image database, medical imaging system etc. [6] The enormous growth in technology in the recent decades has relentlessly promoted the rapid escalation of communication networks. This has inevitably made easy the capturing and dissemination of multimedia over these networks.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

Concomitantly the privacy and the security of information get intricate. The nature of information content stipulates varied methods to protect its secrecy from unauthorized access. As cryptography facilitates storing and transmitting sensitive information over insecure communication networks, it has become one of the most important security measures ever in protecting information.

Cryptography, the science of secret communication, has been practiced in miscellaneous forms for a very long time. Unlike the days when its application was restricted to defence operations and other vital services, today it is pervasive in all digital communication equipment, with security mechanisms in place for secure information transmission from one source to another. Its objective is to prevent adversaries, intruders and eavesdroppers form gaining access to information. A cryptosystem maps the information in a domain to itself. Encryption and decryption are the two processes involved in a cryptosystem. The process of converting intelligible information into unintelligible form is known as encryption and the process in reverse is called decryption. [10] Both the processes require a procedure to be followed with a key. [11] Kerkhof's doctrine (Droge brick & Benedetta 2002) states that "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge".

[17] The two basic types of cryptosystems are symmetric (privatekey) cryptosystem and asymmetric (public-key) cryptosystem. In the symmetric cryptosystem a completely secure secret key is shared between those who intend to communicate, and both encryption and decryption are carried out using the same. Whereas, in the asymmetric cryptosystem there are two keys: one public and the other private. The public-key, is made available to anybody for encryption and the private-key is known only to the intended recipients for decryption. [22] The information encrypted with the public key can be decrypted only with the private key. The goal in designing a cryptosystem is to make encryption and decryption operations inexpensive but ensure that any successful cryptanalytic operation is too complex to be economical (Differ & Hellman 1976).

While designing an encryption algorithm, two general principles are to be considered (Shannon 1949): diffusion and confusion. Diffusion refers to spreading out the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext (Tokarev 2001). That is, a change in a character of the plaintext should influence a change in several characters of the ciphertext and vice versa. Confusion refers to the use of transformations that complicate the dependence of ciphertext statistics on plaintext statistics. Further, according to Schneider (1994), the design objective of a cryptosystem is stated to be as follows, "A 1-bit change of key should produce a radical change in the ciphertext using the same plaintext, and a 1-bit change of the plaintext should produce a radical change in the cipher-text using the same key". This is called the avalanche effect.

1.CHAOS AND CRYPTOGRAPHY[28][33][32]: Chaos is a deterministic non-linear dynamic process that reflects randomness in behaviour and is sensitive to the initial condition (Batterman 1993). There exists an interesting association between chaos and cryptography (Brown & Chua 1996). Many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems (Alvarez & Li 2006). Chaotic systems have several key features that are favourable to secure communications (Behnia et al. 2008), such as ergodicity, sensitivity to initial conditions

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

and control parameters, and random-like behaviour. The most prominent feature is sensitivity to initial conditions and parameters (Jakubowski & Tokarev 2001), and both are invertible dynamic systems (Brown & Chua 1996). Shannon's (1949) discussion on stretching and folding is eminent in chaos theory (Devaney 1989).

2.IMAGE ENCRYPTION: In recent times the security of multimedia (Li et al. 2009), especially images has received much attention, owing to its widespread application in communication networks. Images depict information directly and clearly. [36] An image can be perceived as an arrangement of pixels, and the perceptual information is portrayed intelligible due to the correlation among the adjacent pixels. An image is encrypted by making the adjacent pixels uncorrelated and thereby hiding the information present in it. The traditional text encryption scheme cannot be implemented as such for protecting images, due to its bulk and the presence of redundant data. So, designing a secure image encryption scheme has been a focal research topic since the 1990s.

3.Chaos in Image Encryption: Some built-in features of images restrict the application of conventional encryption algorithm on them. Among the main obstructions is the need for swiftly shuffling and diffusion. [33] It is difficult to achieve this by the means of traditional cryptography, whereas chaos-based algorithms have shown better performance. The random number sequences generated using chaotic maps are deterministic and reproducible. Also, with negligible variation in the initial conditions, chaotic maps can produce diverging results. Hence practically chaos can be used for image encryption.

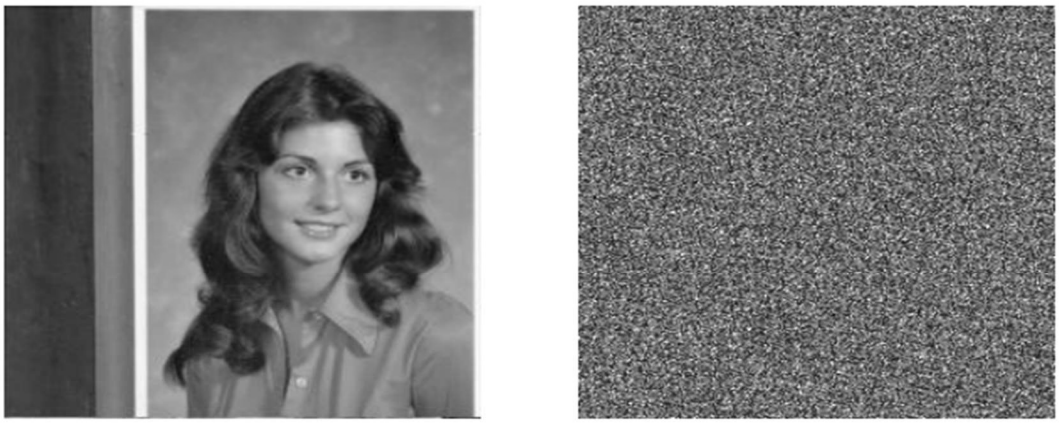
4.A SURVERY OF IMAGE ENCRYPTION TECHNIQUES :

The two main approaches to designing chaos-based cryptosystems (Alvarez & Li 2006) are analogy and digital. [21] Digital chaos-based cryptosystems can be classified into stream ciphers and block ciphers where pixels are encrypted one-by-one and in blocks respectively.

The proposed diffusion technique comprises both permutation and encryption in order to achieve double-image encryption. [37] The scrambled image (The plain image and the scrambled image ($k = 2$, $m = 9$) are presented in Figure 5.3),

5.1-resultant of the BMPP- is sliced into eight bit planes which are depicted in Figure 5.3. The images are presented in order from the 1st bit plane to the 8th bit plane

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342



(a) (b)

Figure 5.3 (a) Plain image (b) Scrambled image

The bit planes shown in Figure 5.3 (i) to (p) are then subjected to the BMPP individually (k = 2, ni = 1, 9, 6, 1, 3, 5, 10, 10, 1 8) and the image is reconstructed by uniting the permuted bit planes in the same order. This process changes the value of the pixels, as the permutation of the bit planes results in a change in the bit positions. This can be observed from the histograms presented in Figure 5.5 for both the scrambled image and the partially encrypted image. It is termed partial encryption, as one more encryption phase is to be carried out

The reconstructed image is again encrypted, using the keys generated by the GDM described in Section 5.3 with Equations (5.4) and (5.5).

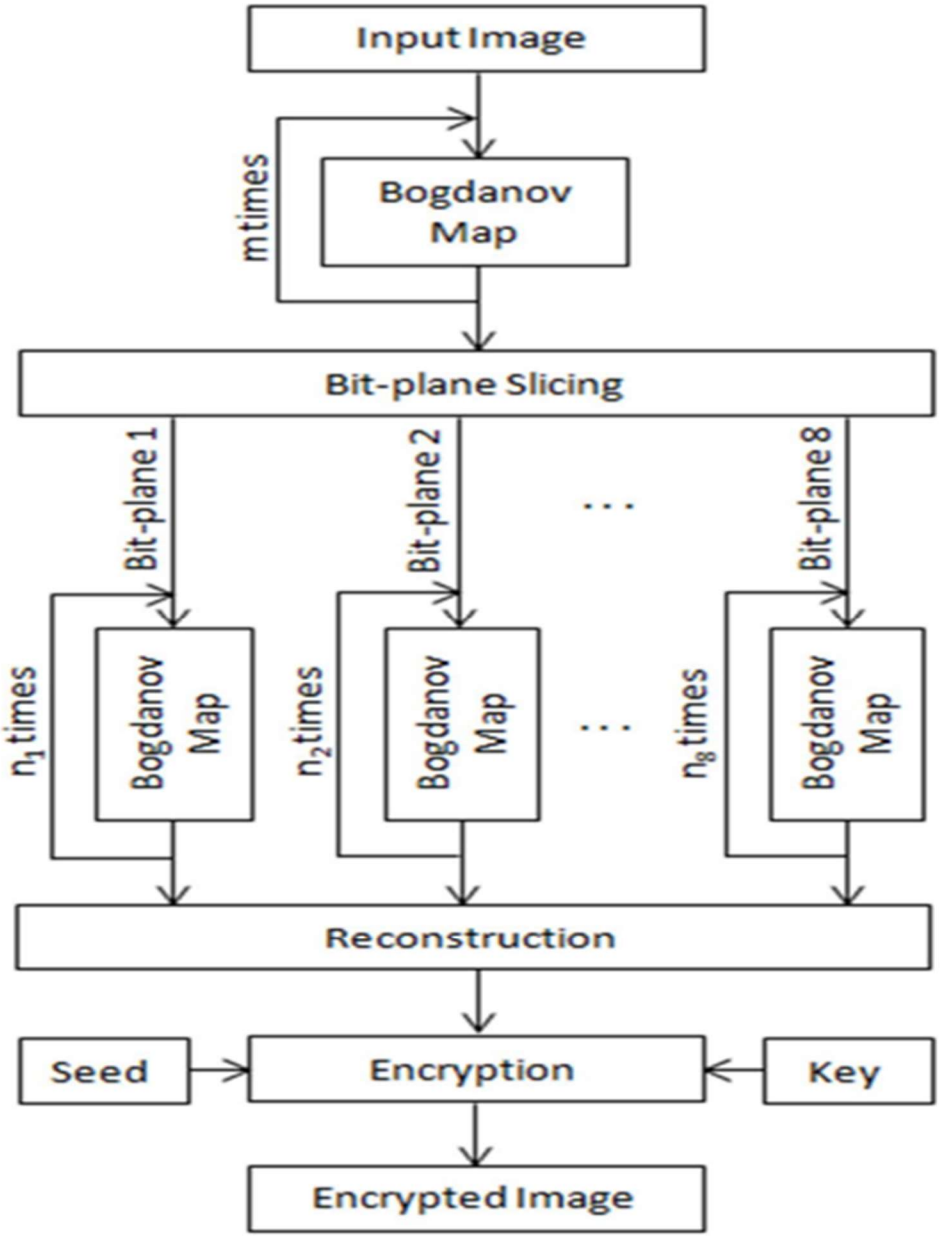
The map x_t+1 = ∇)x_t) yields a random number sequence $\{x_t\}$, once an initial value x0 is given. Further, each pixel of the image is encrypted by considering both the current pixel and the immediate pixel prior to it that is already encrypted. In trying to make the encryption more secure, it must be noted that a change in a pixel may influence the rest of the pixels in the image. [36,33]This is performed by the XOR with mod operation. To generate the initial value, one more variable, s, a seed in the range [0, 255] is random generated. The diffusion operation and inverse operation are performed using the formulas defined in Equation (1) and (2) respectively (Chen et al. 2004). (3)

c(t)=k(t)≤ $[i(t) + k(t)\ mod\ g \leq c(t-1)$…(5.1)

d(t)=[k(t)≤ $c(t) \leq c(t-1) + g - k(t)\ mod\ G$….(5.2)

where I, C, and D are the original image, encrypted image or cipher image, and decrypted image respectively, K is the key sequence and G is the value of the color levels. To compute the initial values of the encrypted and decrypted images, C(0) is set with the value of s, the seed.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342



Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

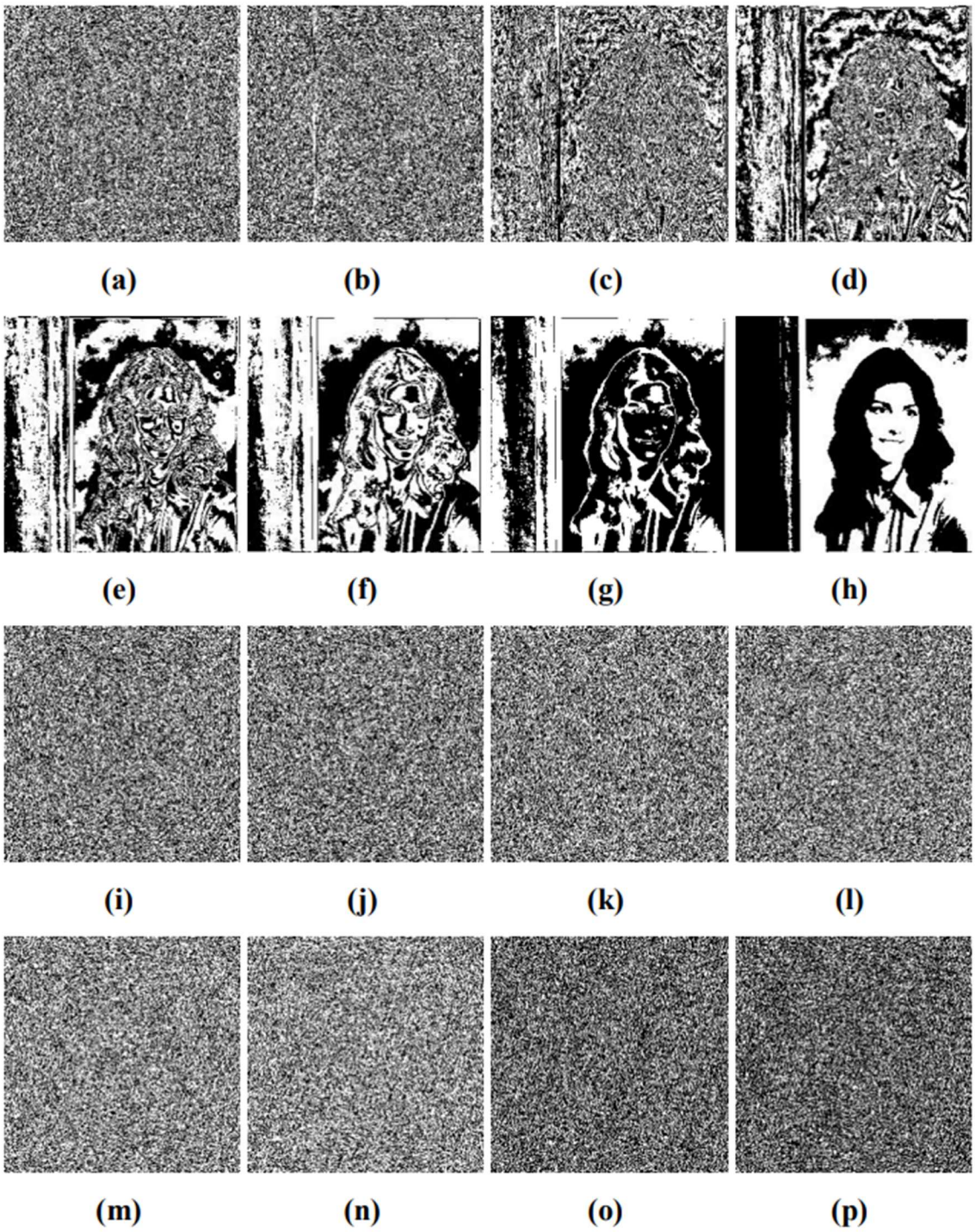


Figure 5.4 Bit planes of (a - h) the plain image and (i - p) the scrambled image

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

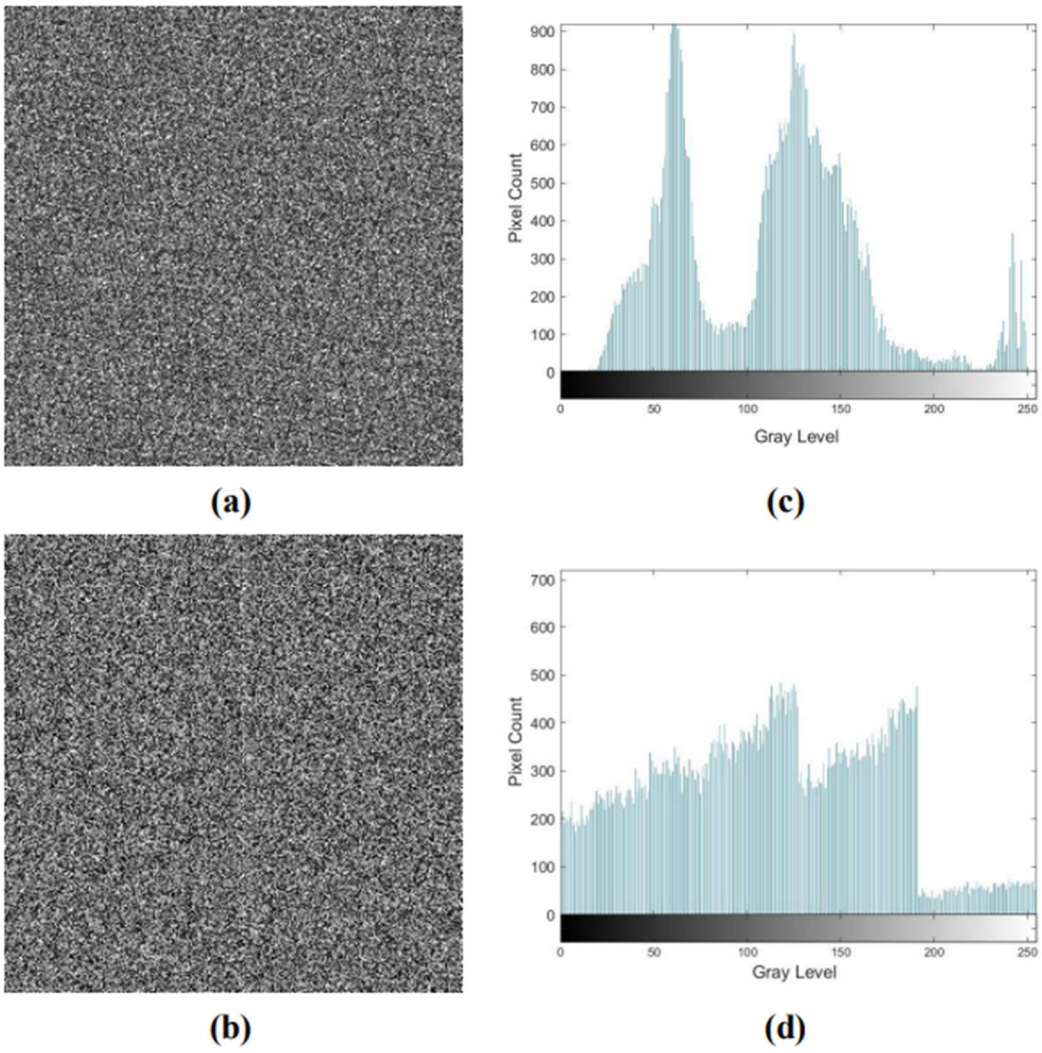


Figure 5.5 (a) Scrambled image (b) Partially encrypted image (c, d) Histograms

Encryption Algorithm The image encryption procedure is shown in Figure 5.6. Consider an image, [9],[3] I, of size M u N. Subject I to the BMPP m times to jumble the position of the pixels, a process that renders the image indecipherable. Let this image be S. Slice S into eight bit planes, Bi , 1 8, and subject each Bi to the BMPP ni times to get φ0 . Then, unite φ0 , 1 8 in order to construct Cp, the partially encrypted image. To perform the chaos-based encryption, the following are to be generated: (i) at random, the value of x0, (ii) a random number key sequence, K, of length MN based on the GDM using Equations (5.1) and (5.2) and a random seed s 255 ,0 [□[. Encrypt S with the key, K, to produce the encrypted image C. [27] The procedure to be carried out for the same is described below .

INVESTIGATION METRICS [11],[30] **:** The performance of the developed speech encryption system has been examined using the following analyses:

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

- Histogram analysis
- Spectrogram analysis
- Correlation analysis Signal to Noise Ratio (SNR)
- Peak Signal to Noise Ratio (PSNR) analysis
- Segmental signal-to-Noise-Ratio (SNR) analysis
- Frequency-Weighed Signal-to-Noise Ratio (FWSNR)
- analysis Key space and key sensitivity analysis
- Number of Samples Change Rate (NSCR) analysis and
- Unified Average Changing Intensity (UACI) analysis.

Histogram Analysis : This analysis is applied to access the invulnerability against Brute force attack (Loizou P.C et al. 2008). In the histogram plot of original signal, the speech samples are distributed at various amplitude levels. In the same manner histogram for encrypted and decrypted speech signal are also plotted. The histogram of decrypted speech signal is identical to the histogram of input speech signal. The histogram of encrypted speech signal is fully masked. The distributions of samples are widely distributed over the space. Hence the frequency attack is impossible in this case.

Spectrogram Analysis : The spectrogram of a speech signal is effective as it divides the speech signals in time domain into multiple blocks (F. Poza et al. 2005; Robert C. Maher, 2009)[28]. FFT is plotted for each block and displayed in the same graph. The spectrograms in respect of original, encrypted and decrypted speech signals are presented. It can be easily noticed by comparing the spectrograms of original speech signal and encrypted speech signal which are completely different as it shows higher encryption quality. Accordingly, by comparing spectrograms of the original speech signal and decrypted speech signals, it is learnt that the original and decrypted speech signals are identical, and thus the decryption quality is proved in terms of better quality.

Correlation Analysis [22] : Correlation analysis is applied to evaluate the statistical relationship between the input speech signal Vs encrypted signal and input signal Vs recovered signal. Normally the range of correlation coefficient will be between +1 and -1. If there is no relationship between the two signals then the correlation coefficient will be closer to 0 otherwise it may be closer to +1 which indicates possible strongest +ve correlation and -1 which indicates possible strongest -ve correlation (Ma J et al. 2008; Vidya Sawant et al. 2017).

SNR Analysis: [13] One of the traditional used objective measures for speech quality is SNR (L. Kocarev, 2001). This analysis is conducted between the original speech signal and the decrypted speech signal to analyze the quality of decrypted speech.

$$SNR = 10\log_{10}\frac{\sum_{n=1}^{N} x^2(n)}{\sum_{n=1}^{N}|x(n)-y(n)|^2}\ [dB] \quad \ldots(1.1)$$

where N is the number of samples, x (n) is the input speech and y(n) is the decrypted speech.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

Peak Signal to Noise Ratio (PSNR) Analysis[14] : PSNR is the ratio between the maximum possible value of an input speech signal and the value of scrambled signal that influences the quality of its representation (A K. Gulve et al., 2014; Harjinder Kau et al., 2012). The maximum probable power of input speech signal against the decrypted signal is reckoned .

$$PSNR = 10\log_{10}\frac{R^2}{MSE} \quad \ldots (1.2)$$

where MSE is the Mean Square Error and R is the maximum variation in the original speech signal. The MSE for input and encrypted streams which are stored in vectors x and y, is computed as

$$MSE = \frac{1}{N}\sum_{i=1}^{n}(x[i]-y[i])^2 \quad \ldots. (1.3)$$

where x(i) is input speech signal, y(i) is encrypted speech signal, N is number of samples.

Segmental Signal to Noise-Ratio (SNRseg) Analysis : [27] For wide range of distorted speech signal Segmental SNR is preferred as a better speech quality measure (S. N. Al-saad et al. 2013). While SNR is calculated for the entire signal, the SNRseg is reckoned with short segments of input signals. Energy fluctuates as speech go by. When speech energy on the higher side, the noise gets inaudible and vice versa.

$$SNRseg = \frac{10}{M}\sum_{m=0}^{M-1}\log_{10}\frac{\sum_{n=Lm}^{Lm+L-1}x^2(n)}{\sum_{n=Lm}^{Lm+L-1}|x(n)-x'(n)|^2} \quad \ldots (1.4)$$

where M represents the number of segments in the signal and L represents the length of the segment.

Robustness Test: NSCR and UACI Analysis The Low Significant Bit (LSB) of input speech signal is changed one bit and converted into an errant speech (Rafik Hamza et al. 2017). [11],[31]Thereafter the input speech signal and the reformed speech signals are encrypted to generate two ciphered speech signals. These two signals are compared to measure NSCR and UACI values. The equation of NSCR is specified below;

where x and y are the two ciphered speech signals. The principle values for NSCR and UACI are 99.9% and 33.3% respectively.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

Table 1.1 Acceptable Rangeof Performance Metrics

S.No	Performance Metrics	Acceptable range as per NIST statistical test suite
1	Histogram Analysis (Loizou P.C et al. 2008)	Original speech – Non-uniform Encrypted speech – Uniform Decrypted speech – Non-uniform
2	Correlation Analysis (Ma J et al. 2008; Vidya Sawant et al. 2017)	-1 to 1
3	SNR in dB (L. Kocarev, 2001)	80dB and above for chaotic noise content
4	PSNR in dB (A K. Gulve et al., 2014; Harjinder Kau et al., 2012)	20dB and above for chaotic noise content
5	SNRseg in dB (S. N. Al-saad et al. 2013)	80dB and above for chaotic noise content
6	fwSNRseg in dB (C. H. Taal et al. 2011)	400dB and above for chaotic noise content
7	Histogram variance (T.Gopalakrishnan et al. 2017)	15% to 40% fluctuation in key variance
8	NSCR (Rafik Hamza et al. 2017; Lima et al. 2016).	Close to 99.9%
9	UACI (Rafik Hamza et al. 2017; Lima et al. 2016).	Close to 33.3%

CHAOTIC MAPS AND CHAOTIC SYSTEM :

Chaos refers to a "state of total confusion with no order" [1],[3] (Cambridge dictionary). Shannon, 1949 proposed a cryptography model based on chaos for symmetric key encryption. The average information theory of chaotic maps was introduced by Kolmogorov and his team (Arnold et al., 1968; Lasota et al. 1994; Katok et al. 1995). Chaos theory is the modern mathematical model in which the behaviour of high sensitive dynamical systems for initial conditions is analysed (Alvarez et al. 1997; Alvarez etal.2003). [7],[14],[22] The dynamic behaviour of the chaotic system does not provide clue to predict and is more reliable (Zeghid et al. 2007). A small change in initial conditions and controlling variables make the system behaviour entirely different. Chaotic system is presented in figure 1.2.

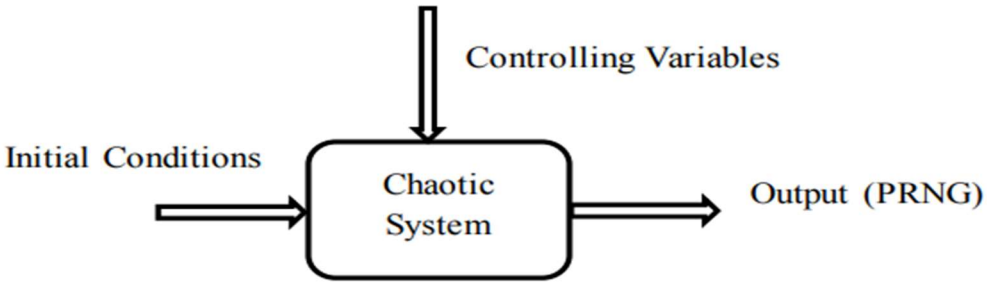
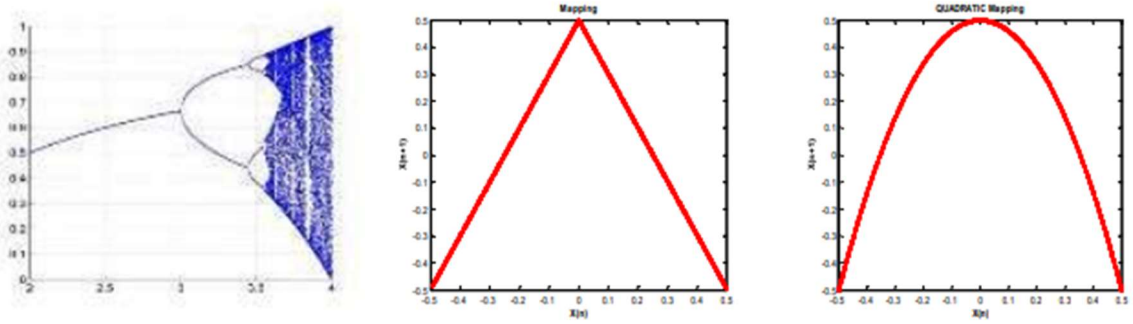


Figure 1.2 Block diagram of Chaotic System

Chaotic maps are classified based on its dimensions, discrete or continuous, real or complex or rational, number of parameters used, etc. One dimensional chaotic maps are Tent map, Logistic map, Circle map, Complex quadratic map, Gauss map, etc. Two dimensional maps are 2D Lorenz system, Arnold's cat map, Baker's map, Exponential map, Hénon map, Lozi map, Zaslavskii map, etc. Three dimensional maps include Sprott chaotic system, Rayleigh-Benard chaotic oscillator, Moore-Spiegel chaotic oscillator, 3D Lorenz system, Chua circuit, Chen chaotic attractor, etc.



Substitution process is added to change the amplitudes of samples in each block. Each sample value is changed by logic operation with mask key value.

Example:

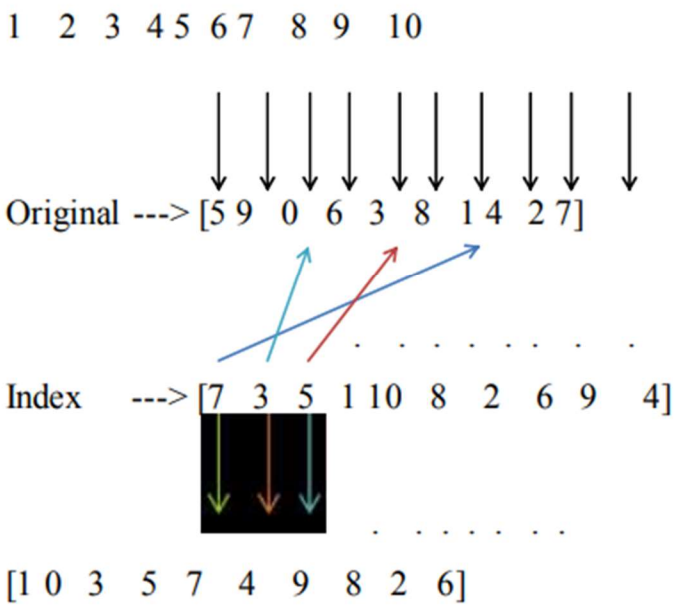
Input speech sample sequence = [5 9 0 6 3 8 1 4 2 7]

Chaotic random number sequence = [3 6 1 9 2 7 0 5 8 4]

Sorted random number sequence = [0 1 2 3 4 5 6 7 8 9]

Position of sorted CRN sequence = [7 3 5 1 10 8 2 6 9 4]

Shuffling the original sequence with respect to the above index:



Piecewise linear chaotic map: [32],[33] Piecewise linear chaotic map (PWLCM) is used as it has ample non linear dynamic action and a positive Lyapunov exponent as shown in Fig. 3. The multi-segmented map shows some fantastic dynamic properties like uniform invariant density function, large positive Lyapunov exponent, and random like behaviour. These properties are particularly valuable and useful for cryptographic purposes. A piecewise linear chaotic map is given by: Here $x0 \in [0, 1)$ is the initial state/initial condition and $m \in (0, 0.5)$ is the control parameter of chaotic map (3). [7] The output of PWLCM has uniformly continuous distribution, confusion and ergodicity. It can also be used to generate good chaotic sequences for making strong S-boxes.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

$$x_{n+1} = f(x_n, m) = \begin{cases} \dfrac{x_n}{m} & \text{if} \quad 0 \le x_n < m \\ \dfrac{x_n - m}{0.5 - m} & \text{if} \quad m \le x_n < 0.5 \\ \dfrac{1 - m - x_n}{0.5 - m} & \text{if} \quad 0.5 < x_n < 1 - m \\ \dfrac{1 - x_n}{m} & \text{if} \quad 1 - m \le x_n < 1 \end{cases} \tag{3}$$

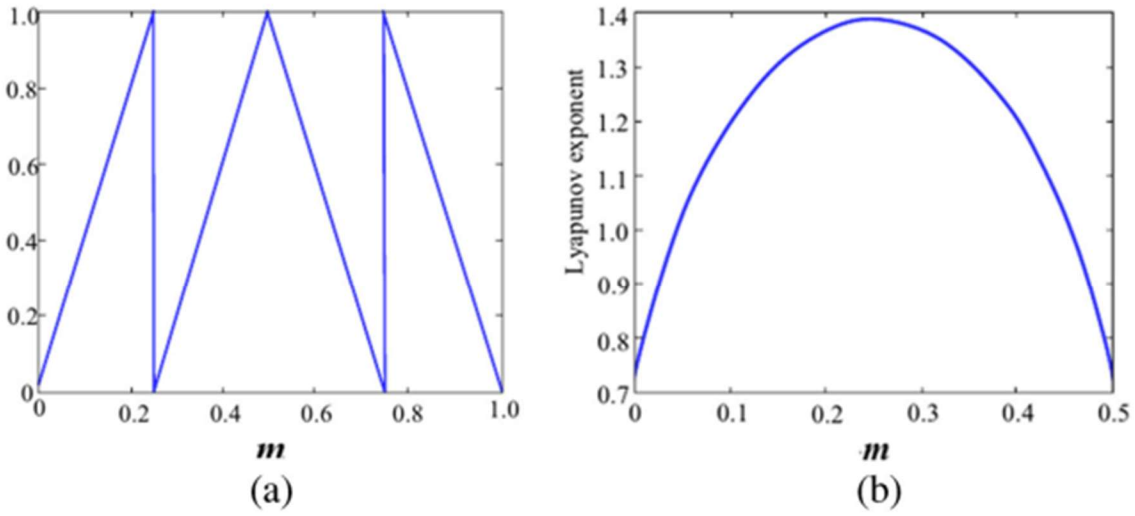


Fig. 3 **a** plot of piecewise linear chaotic map, **b** Lyapunov exponent

The tent logistic system For the solution of problems faced by logistic and tent maps, suggested a new compound chaotic system by bringing together the tent and logistic map. Hence formed new system is named as tent logistic system. The mathematical form of this system can be presented as:

$$x_{n+1} = \begin{cases} \dfrac{4(9-\mu)}{9}(x_n)(1 - x_n) + \dfrac{2\mu}{9}(x_n) & x_n < 0.5 \\ \dfrac{4(9-\mu)}{9}(x_n)(1 - x_n) + \dfrac{2\mu}{9}(1 - x_n) & x_n \ge 0.5 \end{cases}$$

Where $\mu \in [0, 9]$ is the system parameter of the chaotic map (4). For $\mu = 0$ the above equation behaves like logistic map, while for $\mu = 9$ the above described equation degenerates to form the tent chaotic map. [11],[22],[14] Due to this both the logistic and tent chaotic maps can be considered as the special cases of this system. Figure 4 shows the bifurcation and state distribution diagram of said chaotic system. From this figure it is evident that the whole range $\mu \in [0, 9]$ has chaotic behavior, also this chaotic region is much greater than the logistic and tent map. The output of this system is uniformly distributed within [0, 1] This chaotic system is more suitable for the use in cryptographic application as it provides a large chaotic range. Also if the control parameter is used as the secret key key space for the generation of random chaotic sequences, then this key

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

space would be much large to resist brute force attacks. The output random sequence is uniformly distributed to give a good uniformly distributed random sequence.

Example 1 [36] **:** For image encryption we have selected the standard Lena 200×250 image. The original Lena image shown in the Fig. 8a is encrypted by using the proposed Algorithm 3. The resulting encrypted image is visible in Fig.b. The figure shows that the proposed encryption mechanism completely scramble the original image without leaving any clue to reveal the original information. The decryption is then performed by using the proposed image decryption Algorithm 4 and displayed in Fig. c. The decryption result indicates that the proposed scheme effectively works and perfectly recover the original image.

Example 2 [36] **:** In the next example we have taken a Pepper 200 × 250 image. The original image is shown in Fig. a, the encryption result is displayed in Fig. b. The encryption result signifies that the proposed technique generates a noise like structure that does not reveal any useful information about the original image. The decryption result using Algorithm 4 is presented in Fig. 9c. From the decryption result it is evident that the proposed scheme is able to give a flawless recovery.

Algorithm :

1 (Pseudo Random Number Generator (PRNG)) Given the chaotic map

(4), we construct a PRNG by executing the following steps.

1. Set system's control parameter μ, the initial value x0, the positive integer n0 and the L the length of generated sequence.
2. Iterate the chaotic map (4) for L to get a random sequence.
3. Discard first n0 values of above generated sequence to get rid of the harmful effects of transient process.
4. Use a non linear transformation (5) to convert the obtained random sequence X into integer sequence Y, y_i = mod(floor(x_i × 1014), 256), i = 1, 2, ..., (L − n0), (5) where mod gives back the remainder after dividing by 256, while the floor(x) returns the largest integer less than or equal to x. Hence the output sequence

Y = [y1, y2,...,y(L−n0)] lies in the range of [0, 255].

5. Convert each yi to binary number of size 8 bit. Hence a bit sequence is formed that is B = {b1, b2,...,b8(L−n0)}.
6. Change the bit sequence to a single stream of length 100 × 106 bits.
7. Divide the bit sequence to 100 sub sequences, of length 106 bit each. By using the above algorithm we have generated 100 sub sequences, each of length 106 bits.

These sequences are input in NIST statistical suite for their randomness and the obtained results are depicted in the Table 1. The obtained results shows that the sequences generated

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

Table 1.2 Statistical randomness tests results

Test #	NIST statistical test name	p. value	Pass Rate	Result
1	Frequency (monobit)	0.911413	99/100	✓
2	Block Frequency ($m = 128$)	0.897763	99/100	✓
3	The Run Test	0.202268	100/100	✓
4	Cumulative Sums (Forward)	0.637119	100/100	✓
5	Cumulative Sums (Reverse)	0.779188	100/100	✓
6	Longest Run of Ones	0.897763	98/100	✓
7	Non Overlapping Template ($m = 9$, $B = 000000001$)	0.045675	99/100	✓
8	Overlapping Template ($m = 9$)	0.834308	99/100	✓
9	Rank	0.401199	100/100	✓
10	DFT Spectral	0.574903	98/100	✓
11	Universal Statistical Test	0.236810	98/100	✓
12	Approximate Entropy ($m = 10$)	0.574903	99/100	✓
13	Random Excursions	0.554420	57/57	✓
14	Random Excursions Variant	0.474986	56/57	✓
15	Serial ($m = 16$)	0.935716	99/100	✓
16	Linear Complexity ($M = 500$)	0.090936	100/100	✓

from tent logistic chaotic map pass almost all the tests. Hence tent logistic map can be used as a potential platform for the generation of a good chaotic random sequence

SCOPE OF THE PAPER -Escobar & Cruz-Hernandez (2017) have stated that the effectiveness and performance of low-dimensional chaotic systems have a significant role in the hardware implementation of cryptosystems, and can be employed to generate the random number key sequence used for image encryption. Amending and augmenting these systems to improve their adaption to image encryption has been a focused area of research. The work presented in this thesis use one- and two-dimensional (1D and 2D) chaotic maps. The confusion techniques proposed in this thesis are based on 2D maps such as the Arnold cat map and the Bogdanov map, whereas the diffusion techniques proposed in the thesis are based on 1D maps such as the doubling map and SOM maps. Because of their simple construction, discrete nature, fewer arithmetic operations, high yield and simple implementation in digital systems, they are used in image encryption.

MATLAB is used to produce the experimental results. Standard images have been used for encryption during simulation.

Comparison : a deep and detailed overall comparison of the proposed scheme with other image encryption schemes is given below –

Table – 1.3

Algorithms	**NPCR**	**UACI**	**Correlation**	**key space**	**Entropy**
Akkar, ML[10]	93.25	-	0.002518	10^{11}	5.1548
Arribas [17]	91.89	-	0.25481	10^{90}	5.1201

Acharya.B [21]	89.78	31.28	0.00213	10^{77}	5.1225
Husainy&Uliyan[23]	95.79	32.00	0.21546	10^{123}	5.1256
Diaconu, AV [31]	97.29	30.00	0.215846	10^{81}	5.2658
Diffe.W&Hellman[32]	94.00	29.99	0.000124	10^{33}	5.0001
chai et al. [35]	99.63	-	0.0037	10^{51}	7.9983
Tahir Sajjad Ali & Rashid Ali [36]	87.01	33.00	0.00558	10^{37}	5.9912
Wang et al. [37]	99.5956	33.5512	0.0038	10^{56}	7.9975

CONCLUSION : Images have become an intrinsic part of the business, medical, armed forces and social media landscape. This stipulates that cryptosystems be set up for secure transmission of sensitive images through insecure communication networks. Traditional cryptosystems, largely based on number theory, are unsuitable for digital images, given their high data capacity and data redundancy. Also, the correlation between adjacent pixels in a digital image is strong. In recent years, chaos-based image encryption techniques have been used extensively because of certain fundamental properties of theirs such as unpredictability, sensitivity to initial conditions, and ergodicity. The strong relationship between the properties of chaos-based systems and cryptography has helped design a chaos-based cryptosystem with excellent confusion and diffusion processes.

In this paper, a chaos-based cryptosystem for images has been proposed with both confusion and diffusion phases, based on 2D chaotic maps such as the Arnold transform and Bogdanov map, and 1D chaotic maps such as the doubling map and SOM map. The description of the maps and their properties has been discussed, and the implementation and performance of the map-based devised methods presented.

The EAT matrices were formulated from the basic matrices of the general Arnold transform by augmenting them with their mirror matrices. The EAT matrices were used to permute the pixel position of the image. Experimental results showed better scrambling with fewer iterations. The correlation analysis produced a good dispersal of pixels when computed in all the three horizontal, vertical and diagonal directions, and also produced a lesser correlation coefficient, exhibiting the results of uncorrelation among the pixels in the image. The periodicity of the proposed EAT was more than twice that of the Arnold transform, resulting in increased key space. The EAT produced higher values of GDD than the Arnold transform, both in the 4-pixel and 8-pixel neighbourhoods. However, the application of the EAT is limited to square images, as in the case of the Arnold transform.

A theoretical analysis of the 2D chaotic Bogdanov map demonstrated that its application can be extended to image encryption because of its characteristics of automorphism, one-to-one correspondence, and area preservation. The scrambling method, [7,6,2,13] BMPP, was formulated based on the Bogdanov map. Experimental results showed that the BMPP had a good correlation distribution and produced superior scrambling with fewer iterations. The number of scrambling patterns produced grew exponentially with the size of the images, and the numbers of unique

patterns were the same for k being odd or even. However, only when k was even, the periodicity was more than twice that of the Arnold transform, leading to a larger key space. Compared to the Arnold transform, the BMPP produced a higher GDD. The greatest advantage of the BMPP is that it can be applied even on images having unequal dimensions, without subjecting the images to further computation or modification.

REFERENCES :

[1]. Aabid, MAE, Guilley, S & Hoogvorst, P 2007, _Template attacks with a power model‘, Cryptology ePrint Archive, Report, p. 443.
[2]. Acii¸cmez, O, etin Kaya Ko¸ C & Seifert, JP 2007, _On the power of simple branch prediction analysis‘, In ASIACCS ‘07: Proceedings of the 2nd ACM symposium on Information, computer and communications security, New York, NY, USA, 2007.ACM, pp. 312–320.
[3]. Aciicmez, O, Seifert, JP & Koc, CK 2006, _Predicting secret keys via branch prediction‘, Cryptology ePrint Archive, Report, p. 288.
[4]. Aghaie, A, Moradi, A, Rasoolzadeh, S, Schellenberg, F & Schneider, T 2018, _Impeccable Circuits‘, IACR Cryptology ePrint Archive, p. 203.
[5]. Agrawal, D, Archambeault, B, Rao, JR & Rohatgi, P 2002, _The EM sidechannel(s)‘, in 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp. 29–45.
[6]. Agrawal, D, Rao, JR & Rohatgi, P 2003, _Multi-channel Attacks‘, In CHES, pp. 2–16.
[7]. Agrawal, D, Rao, JR, Rohatgi, P & Schramm, K 2005, _Templates as Master Keys‘, In CHES, pp. 15–29.
[8]. Aigner, M & Oswald, E, _Power analysis tutorial‘, Technical report, University of Technology Graz.
[9]. Akkar, ML & Giraud, C 2001, _An Implementation of DES and AES, Secure against Some Attacks‘, In CHES ‘01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems, pp. 309–318, London, UK, 2001. Springer-Verlag.
[10]. Akkar, ML, Bevan, R, Dischamp, P & Moyart, D 2000, _Power analysis, what is now possible... In ASIACRYPT ‘00: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security, London, UK, 2000. SpringerVerlag, pp. 489–502
[11]. Ambrose, JA, Ragel, RG & Parameswaran, S 2007, _A Smart Random Code Injection to Mask Power Analysis Based Side Channel Attacks‘, In CODES+ISSS ‘07: Proceedings of the 5th international conference on Hardware/software codesign and system synthesis, pp. 51–56, New York, NY, USA, 2007. ACM Press.
[12]. Anderson, R, Biham, E & Knudsen, L, _Serpent: A Proposal for the Advanced Encryption Standard‘.
[13]. Ankush Srivastava & Prokash Ghosh 2019, _An Efficient Memory Zeroization Technique Under Side-Channel Attacks‘, 32nd International Conference on VLSI Design.
[14]. Aoki, K, Ichikawa, T, Kanda, M, Matsui, M, Moriai, S, Nakajima, J & Tokita, T 2000, _Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis‘, In Selected Areas in Cryptography, pp. 39–56.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

[15]. Archambeau, C, Peeters, E, Standaert, FX & Quisquater, JJ, _Template Attacks in Principal Subspaces‘, In CHES, pp. 1–1.
[16]. Arooj Nissar & Mir, AH 2010, _Classification of stage analysis techniques: A study‘, Digital Signal Processing, pp.1758–1770.
[17]. Arribas, V, Bilgin, B, Petrides, G, Nikova, S & Rijmen, V 2018, _Rhythmic Keccak: SCA Security and Low Latency in HW‘, IACR Transactions on Cryptographic Hardware and Embedded Systems 2018, vol. 1, pp. 269–290.
[18]. Arribas, V, Cnudde, TD & Šijačić, D 2017, _Glitch-Resistant Masking Schemes as Countermeasure Against Fault Sensitivity Analysis‘, In FDTC IEEE Computer Society, pp. 1–8.
[19]. Aarthi, R & Kavitha, S 2017, ‘Image encryption using binary bit plane and rotation method for an image security’, Internationall Journal of Engineering Development and Research, vol. 5, no.
[20], pp. 2321-9939. 2. Abbas, NA 2016, ‘Image encryption based on independent component analysis and Arnold’s cat map’, Egyptian Informatics Journal, vol. 17, no. 1, pp. 139-146.
[21]. Acharya, B , Patra, SK & Panda, G 2008, Image encryption by novel cryptosystem using matrix transformation : First International Conference on Emerging Trends in Engineering and Technology , pp. 77-81.
[22]. Adda, AP , Jadj-Said, N , M’Hamed, A & Belgoraf, A 2007, ‘Lorenz’s attractor applied to the stream cipher’, Chaos, Solitons & Fractals, vol. 33, no. 5, pp. 1762-1766.
[23]. Al-Husainy & Uliyan, DM 2017, ‘Image encryption technique based on the entropy value of a random block’, International Journal of Advanced Computer Science and Applications, vol. 8, no. 7, pp. 260-266.
[24]. Al-Romema, NA , Mashat, AS & AlBidewi, I 2012, ‘New chaos-based image encryption scheme for RGB components of color image’, Computer Science and Engineering, vol. 2, no. 5, pp. 77-85.
[25]. Alvarez, G & Li 2006, ‘Some basic cryptographic requirements for chaos-based cryptosystems’, International Journal of Bifurccation and Chaos, vol. 16, no. 8, pp. 2129-2151.
[26]. Arrowsmith, DK , Cartwright, Lansbury, AN & Place, CM 1993, ‘The Bogdanov map: Bifurcations, mode locking and chaos in a dissipative system’, International Journal of Bifurcation and Chaos, vol. 3, no. 4, pp. 803-842.
[27]. Arroyo, D, Li, Amigo, JM, Alvarez, G & Rhouma, R 2010, ‘Comments on "Image encryption with chaotically coupled chaotic maps"‘, Physica D: Nonlinear Phenomena, vol. 239, no. 12, pp. 1002-1006.
[28]. De Monte, S, d’Ovidio, F, Chate, H & Mosekilde, E 2005, ‘Effects of microscopic disorder on the collective dynamics of globally coupled maps’, Physics D: Nonlinear Phenomena, vol. 205, no. 1-4, pp. 25-40.
[29]. Denning 1982, Cryptography and data security, Addison-Wesley Publishing Company, Inc, USA.
[30]. Devaney, RL 1989, An Introduction to Chaotic Dynamical Systems, Addison-Wesley, California.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 324-342

[31]. Diaconu, AV, Costea, A & Costea, MA 2014, 'Color image scrambling technique based on transposition of pixels between RGB channels using knight's moving rules and digital chaotic map', Mathematical Problems in Engineering, vol. 014, p. 15 pages.

[32]. Diffe, W & Hellman, ME 1976, 'New Directions in Cryptography', IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654.

[33]. Wang X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics Lasers Eng 107:370–379

[34]. Wu Y, Noonan JP, Again S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Select Areas Telecommand (JSAT) 1(2):31–38

[35]. Chai X, Bi J, Gan Z, Liu X, Zhang Y, Chen Y (2020) Colour image compression and encryption scheme based on compressive sensing and double random encryption strategy. Sig Process 176:107684

[36]. Tahir Sajjad Ali & Rashid Ali, Multimedia Tools and Applications (2022) 81:20585–20609 A novel colour image encryption scheme based on a new dynamic compound chaotic map and S-box. under exclusive licence to Springer Science + Business Media, LLC, part of Springer Nature 2022.

[37]. Wang X, Zhu X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics Lasers Eng 107:370–379

[38]. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ELGamal scheme. Sig Process 141:109–124