2024, 21(5 Special Issue): 1850-1867
https://doi.org/10.21123/bsj.2024.10565
P-ISSN: 2078-8665 - E-ISSN: 2411-7986

Baghdad Science Journal

Analyzing the Efficiency of a New Image Encryption Method Based on Aboodh Transformations

Suresh Rasappan[1], **Regan Murugesan**[2], **Sathish Kumar Kumaravel**[2] **Kala Raja Mohan**[2], **Nagadevi Bala Nagaram**[2]*

[1]Department of Mathematics, University of Technology and Applied Sciences, Ibri, Oman.
[2]Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai – 600062, Tamilnadu, India.
*Corresponding Author.

ICCDA2023: International Conference on Computing and Data Analytics 2023.

Received 02/01/2024, Revised 20/04/2024, Accepted 22/04/2024, Published 25/05/2024

Abstract

The goal of this research is to develop a unique cryptographic method that makes use of Aboodh and its inverse transform in combination with the S-Box approach. The results of evaluations indicate that this work is appropriate for use in safe cryptographic applications, and it provides clues regarding the building of an image cryptosystem based on the complicated behaviors that it demonstrates. After applying the methodologies that have been provided to depict data taken from real-life situations, the results have been evaluated using a wide variety of statistical and performance criteria. The findings of this investigation result in an improvement to the reliability of the cryptosystem.

Keywords: Aboodh Transformation, Cryptography, Decryption, Encryption, S-Box Method.

Introduction

The importance of secure and private data transfer in today's era of preeminent digital communication and information dissemination cannot be overstated. Since the quantity of sensitive information that is being transferred via computer networks is continually growing at a rapid rate, it is of the highest necessity to have solid protection against unauthorized access and interception[1-4]. Cryptography, often known as the art and science of secure communication, is at the vanguard of the struggle to defend the authenticity, integrity, and confidentiality of our digital world. Cryptography is both an art and a science. Mathematical principles and computational theory are brought together in the field of cryptography[5,6]. A Foundational and important overview of cryptography's underlying theories and applications offers a glimpse into the fundamental technology that enables secure digital communication and the protection of sensitive data. The two basic types of keys that are utilized in the process of cryptography are known as symmetric keys and asymmetric keys. The key that is utilized in the process of encrypting and decrypting cypher text is typically referred to as the secret key. This terminology is employed since it is usual practice. When encrypting and decrypting cypher text, symmetric keys only require the usage of a single key. These key shaves been in use for quite some time. Block cyphers and stream cyphers are the two basic categories that secret-key cyphers may be grouped into. Stream cyphers are a subcategory of block cyphers. Block cyphers, on the other hand, apply a private key and algorithm to a data block concurrently, as opposed to stream cyphers, which process the key and algorithm one bit at a time. Block cyphers offer a higher level of protection than stream cyphers do. The great majority of cryptographic processes employ symmetric encryption for the transit of data, whilst asymmetric encryption is utilized for the protection and exchange of the secret key. The procedure of symmetric encryption, which is also known as private key encryption, requires the use of the same private key for both the encryption and decryption processes[7-10]. If the key is either misplaced or stolen by a third party who is not authorized to have it, both of which are probable results of employing this approach, the safety of the system might be compromised, and it would no longer be possible to transmit messages in a secure manner[11-13].

It is common practice to implement encryption and decryption systems with the primary intention of securing the privacy of users. As information is sent across the expansive length of the World Wide Web, it becomes increasingly vulnerable to unlawful access by a diverse range of individuals and institutions[14-17]. Deciphering, the process of converting encoded or encrypted information into a comprehensible form for both humans and machines, can be accomplished manually or electronically[18-20]. Encryption, the reverse process of deciphering, involves scrambling data using a unique sequence of bits, specifically designed for this purpose This special bit sequence, known as an encryption key, is generated using methods that ensure its unpredictability and uniqueness. Encryption transforms plain text data into an unintelligible arrangement of characters called cipher text[21-24]. Decryption, the reversal of encryption, converts cipher text back into its original plain text form. This term encompasses a variety of techniques for manually or digitally decrypting data using appropriate codes and keys.

For message encryption and decryption, a select few authors have developed a suitable function and constructed the outputs in the generalized form using the Laplace transform, as well as their related approach. This was done to facilitate the process of message encryption and decryption. It is impossible to exaggerate the value that a transformation-rich algorithm brings to the table in terms of its ability to change keys and prevent fraud. A significant number of researchers have shown an interest in making use of mathematical techniques in cryptography. Inverse transformations, conformal mapping, and Laplace transformations are only a few of the many ways that may be utilized to bolster the security of cryptographic protocols. The process of encoding and decoding information is better understood because to the mathematical tools at our disposal. The creation of first-order ordinary differential equations is a strategy that scientists have implemented in order to safeguard their work. Using this strategy helps ensure the confidentiality of any data that is being sent or stored. In order to retrieve the original data, the variable separable method is utilized once again. This method makes decryption easier, which in turn makes it possible for authorized people to gain access to the concealed information. Researchers seek to improve the ability of cryptographic systems to safeguard sensitive information by combining mathematical concepts and methods into cryptography[25]. Researchers want to improve the ability of cryptographic systems to protect sensitive information.

Information in plain language is the sort of stuff that must be guarded carefully before it can be translated into any other kind of disguised format. The term “cypher text” refers to text that has been encoded in such a way that it cannot be read in its original form. This prevents the text from being deciphered. It is necessary to make use of the key in order to convert the cipher text into a format that can be read. A unique strategy has been developed that makes use of the Laplace-Mellin transform. This strategy makes use of the key that possesses a multiple-number modulus function in order to solve the problem. As a direct consequence of this, the process has always been an error-free algorithm.

Researchers have shown an increasing curiosity in developing their own S-boxes in recent years by incorporating existing ones into image encryption methods. Recently, a few academics have constructed dynamic S-boxes to increase the effectiveness of picture encryption. In addition to this, they have invented a method of image encryption that takes use of a novel S-box that is produced by a system that is characterized as being hyper-chaotic. This technique has a variety of benefits, including a clear structure, an outstanding encryption performance, and a rapid encryption speed[26-28]. Cryptanalysis is another important field of research that focuses on deciphering encryption keys or searching for cipher text. This contrasts with information encryption, which is primarily concerned with preventing information from being read by

unauthorized parties. Cryptanalysis is useful to the field of cryptography since it pinpoints weaknesses in cryptographic algorithms and contributes to the general advancement of the discipline. In addition to this, it helps to avoid the installation of hazardous encryption techniques in communication that is carried out in the real world, which is another important function it serves.

The article begins with an introduction that delves into the prerequisites for standard cryptographic operations. Subsequently, it presents the methodology employed for encrypting and decrypting images using the Aboodh transformation, which is the technique used in this study. The results and discussion section evaluates the effectiveness of the proposed method, including a data-loss attack and comparative reliability assessment. Additionally, it examines the correlation performance, histogram testing, information entropy, differential analyses, key space analysis, and key sensitivity analysis. Finally, the article concludes with citations.

Preliminaries

The definitions made use of in the process of proposed cryptographic analysis are listed below.

Plain Text, Cipher Text and Cipher

The message that requires secure communication, in its original and unaltered form, is known as the plaintext. To ensure confidentiality, the plaintext undergoes a transformation using a suitable methodology. This transformation changes the plaintext into a different form that no longer resembles the original, making it unreadable to humans. This transformed text is referred to as cipher text. The process of converting plaintext into cipher text using a specific algorithm or method is called encryption, and the algorithm applied for this purpose is known as a cipher. Encryption and ciphers play a crucial role in secure communication and data protection, preserving the confidentiality and security of sensitive information during transmission or storage.

Encryption and Decryption

The art of transforming plain text into unintelligible cipher text, known as encryption, serves as a cornerstone for safeguarding sensitive data from unauthorized access. This process renders the information indecipherable without the possession of the corresponding decryption key. Conversely, decryption, the in- verse operation, unveils the original plaintext from its encrypted counterpart. This process is paramount in extracting the intended message from encrypted data, enabling authorized recipients to securely access confidential information. Encryption and decryption, acting as the bedrock of cryptography, ensure the unwavering confidentiality and security of data during transmission or storage.

Aboodh Transform

Aboodh transform of a function $f(t)$ is given by the Eq. 1.

$$A[f(t)] = \frac{1}{V}\int_0^\infty f(t)e^{-Vt}dt\,, t \geq 0, k_1 \leq v \leq k_2. \quad 1$$

The Aboodh transform of t^n given by Eq. 2.

$$(t^n) = \frac{n!}{v^{n+2}}. \quad 2$$

The Aboodh transform of any constant l given by$(l) = \frac{l}{v^2}$

These two Aboodh transforms are used for the Encryption process in this paper.

Inverse Aboodh Transform

The inverse Aboodh transform used in the decryption process of this paper are as follows and it is represented by the Eq. 3.

$$A^{-1}\left\{\frac{1}{V^2}\right\} = 1 \text{ and } A^{-1}\left\{\frac{n!}{V^{n+2}}\right\} = t^n. \quad 3$$

Cosine Functions

Hyperbolic functions are similar to ordinary trigonometric functions, which are defined using hyperbola.

The expansion of hyperbolic cosine function used for this cryptographic analysis is given by Eq. 4.

$$\cos hx = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots \qquad 4$$

Modulo Operation

The modulo operation, often denoted by the symbol % calculates the remainder when one integer is divided by another. It is a fundamental mathematical operation in number theory and computer programming.

Methodology

Data Encryption and Decryption

Data security is crucial due to the increasing complexity of online activities. Digital images are the com- mon medium for representing data. Digital images can be protected by utilizing image encryption technologies. One goal of image encryption is to render the original image's content unrecognizable[29-31]. Secure image cryptosystems are frequently developed using chaotic models[32-35]. The Aboodh transformation is proposed for use in an image crypto scheme. Therefore, the suggested picture cryptosystem and its performance evaluations are the focus of this section. This prevents hackers from sleuthing out the date in advance. In this part, we'll go over the proposed mechanism for Aboodh transformations-based cryptography and analyze it.

Five images of an airplane, a baboon, a boat, a house, and a pepper were used to evaluate the suggested method. The figures in this article show how the image can be encrypted and decrypted as an example. Data extraction from cipher images is impossible, as demonstrated by the simulation results.

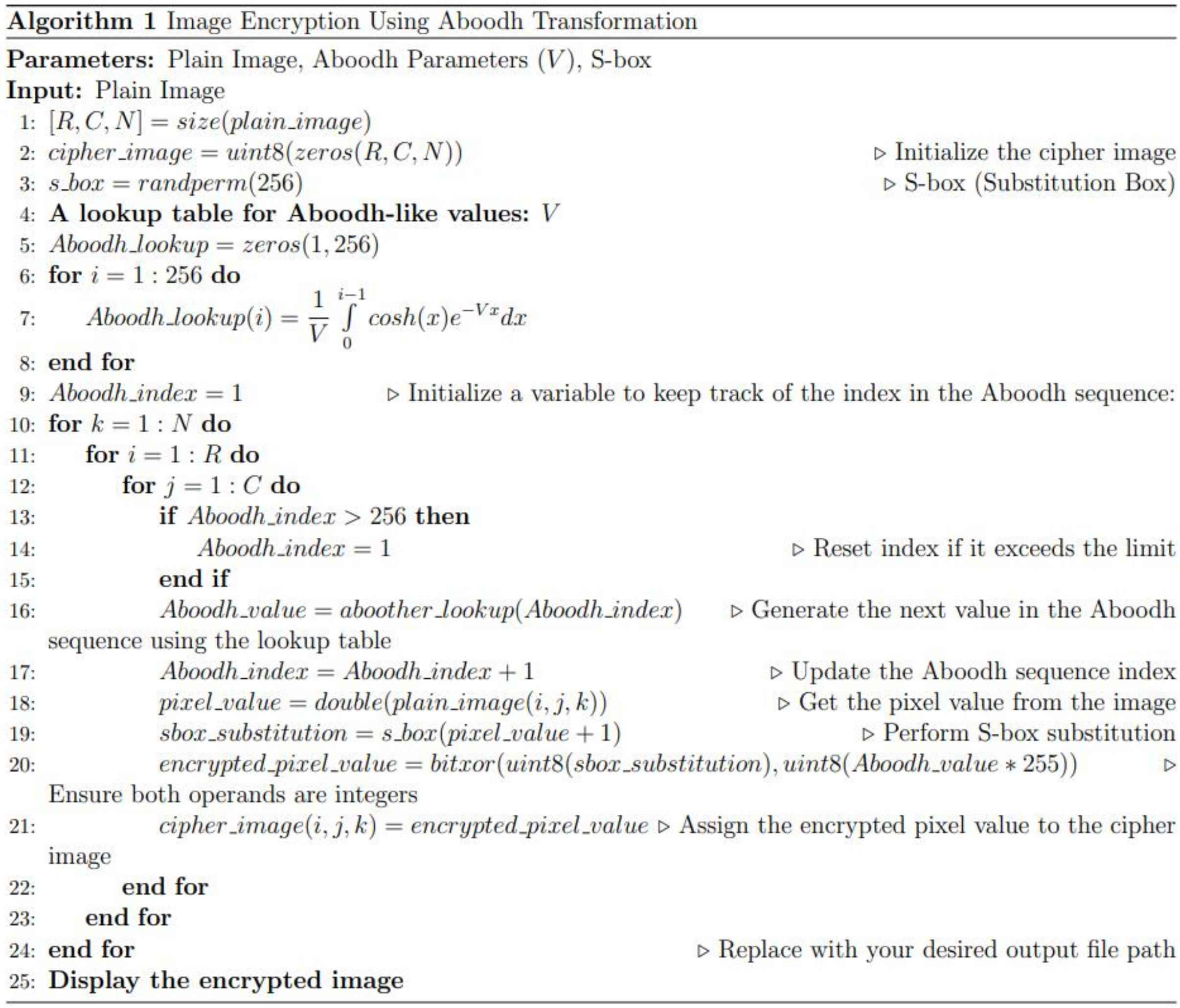
Encryption Algorithm for Image

Encrypting images involves protecting the contents of an image file from unauthorized access by using encryption algorithms. There are different encryption techniques that can be applied to image data, depending on the level of security required and the use case. Here are some common encryption methods for images: Symmetric Key Encryption: Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that can be applied to encrypt image files. You can use AES in different modes, such as ECB (Electronic Codebook), CBC (Cipher Block Chaining), or GCM (Galois/Counter Mode), depending on your specific needs. Asymmetric Key Encryption like Rivest–Shamir–Adleman, can be used for encrypting a symmetric key, which is then used to encrypt the image. This allows for secure transmission or storage of images without sharing the symmetric key.

Hybrid Encryption is a common approach to combine both symmetric and asymmetric encryption. You can use asymmetric encryption to securely share the symmetric key, and then use symmetric encryption like AES to encrypt the image data. Image Steganography is the practice of hiding information within an image. Instead of encrypting the entire image, you can hide sensitive data within the image, making it less obvious that encryption has been applied. Holomorphic Encryption is a specialized technique that allows for operations to be performed on encrypted data without decryption. While it's not commonly used for image encryption due to its complexity, it can be applied to certain use cases. Encryption algorithms are mathematical functions that are used to convert original, plain-image data into encrypted, unreadable cipher-image, and vice versa. The purpose of encryption is to secure sensitive information from unauthorized access by transforming it into a format that can only be read by someone with the proper decryption key.

Chaotic oscillator-based encryption algorithms leverage mathematical models of chaotic systems to generate encryption keys for enhancing the security of digital communications. These algorithms exploit the unpredictable and intricate behavior of chaotic systems to create encryption keys that are challenging for potential attackers to decipher. However, the security of chaotic oscillator-based encryption algorithms is a topic of ongoing research and study.

The proposed image encryption system in this context employs a technique for Aboodh transformation along with the S-Box approach. The sequence created is originally employed for the purpose of substituting the original image. The aforementioned adapted technique is thereafter employed to produce Aboodh sequences for the purpose of reordering the rows of the substituted image, as well as another sequence for reordering its columns. Ultimately, the reorganized components are brought together in order to generate the encrypted image. Algorithm 1 encompasses the entirety of the procedure, delineating the suggested image encryption approach. Understanding the fundamental importance of the encryption key's strength and the algorithm's resilience is crucial in safeguarding sensitive data during digital transmission or storage.

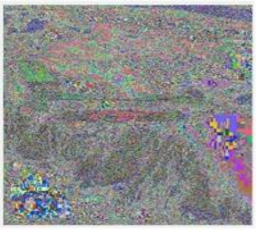


Algorithm 1 Image Encryption Using Aboodh Transformation

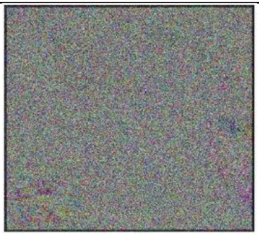
Parameters: Plain Image, Aboodh Parameters (V), S-box
Input: Plain Image

```
$[R, C, N] = size(plain\_image)$
$cipher\_image = uint8(zeros(R, C, N))$        ▷ Initialize the cipher image
$s\_box = randperm(256)$        ▷ S-box (Substitution Box)
A lookup table for Aboodh-like values: $V$
$Aboodh\_lookup = zeros(1, 256)$
for $i = 1 : 256$ do
    $Aboodh\_lookup(i) = \frac{1}{V} \int_{0}^{i-1} cosh(x) e^{-Vx} dx$
end for
$Aboodh\_index = 1$        ▷ Initialize a variable to keep track of the index in the Aboodh sequence:
for $k = 1 : N$ do
    for $i = 1 : R$ do
        for $j = 1 : C$ do
            if $Aboodh\_index > 256$ then
                $Aboodh\_index = 1$        ▷ Reset index if it exceeds the limit
            end if
            $Aboodh\_value = aboother\_lookup(Aboodh\_index)$        ▷ Generate the next value in the Aboodh sequence using the lookup table
            $Aboodh\_index = Aboodh\_index + 1$        ▷ Update the Aboodh sequence index
            $pixel\_value = double(plain\_image(i, j, k))$        ▷ Get the pixel value from the image
            $sbox\_substitution = s\_box(pixel\_value + 1)$        ▷ Perform S-box substitution
            $encrypted\_pixel\_value = bitxor(uint8(sbox\_substitution), uint8(Aboodh\_value * 255))$        ▷ Ensure both operands are integers
            $cipher\_image(i, j, k) = encrypted\_pixel\_value$        ▷ Assign the encrypted pixel value to the cipher image
        end for
    end for
end for        ▷ Replace with your desired output file path
Display the encrypted image
```

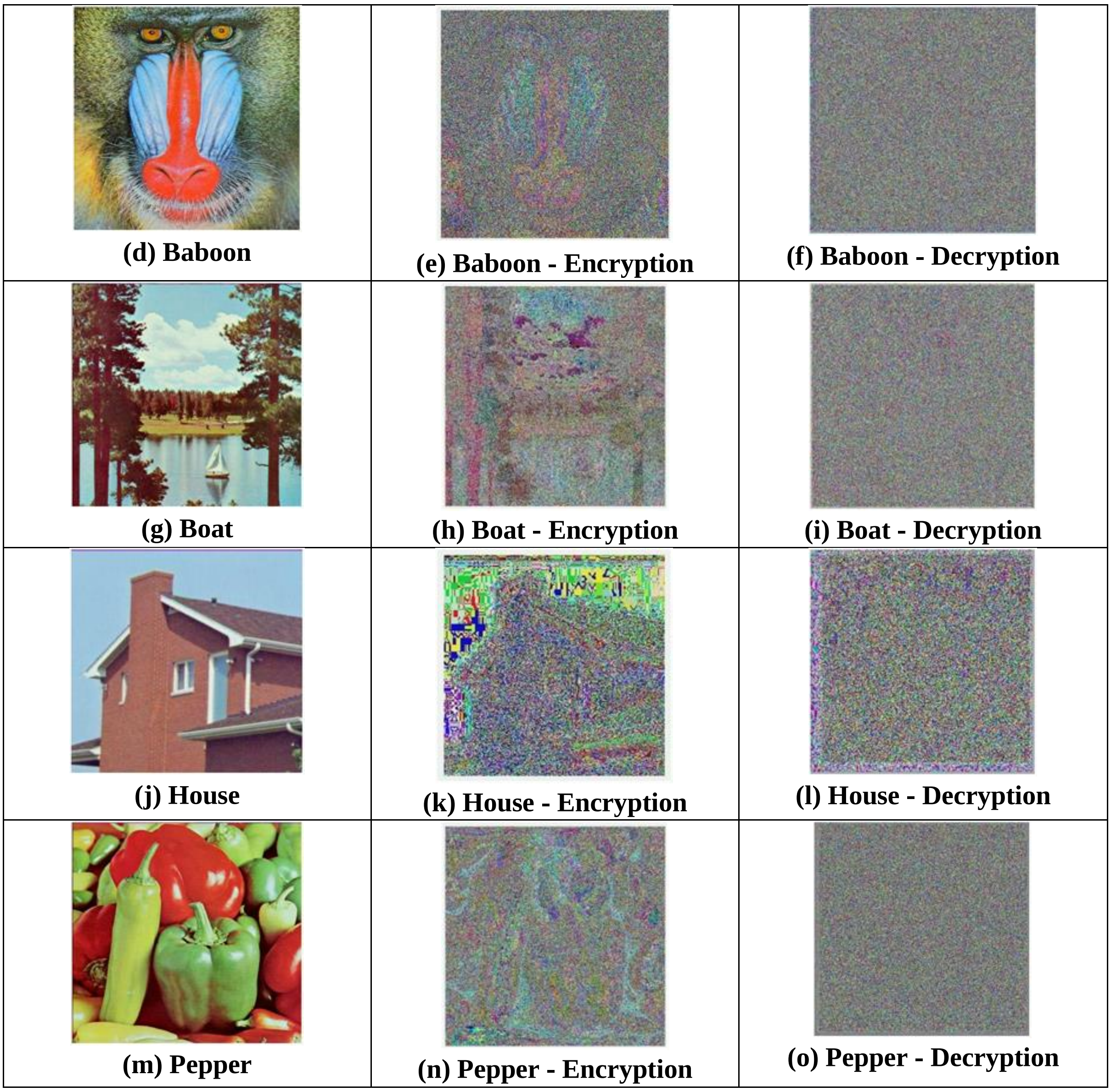
(a) Airplane



(b) Airplane - Encryption



(c) Airplane - Decryption



(d) Baboon **(e) Baboon - Encryption** **(f) Baboon - Decryption**

(g) Boat **(h) Boat - Encryption** **(i) Boat - Decryption**

(j) House **(k) House - Encryption** **(l) House - Decryption**

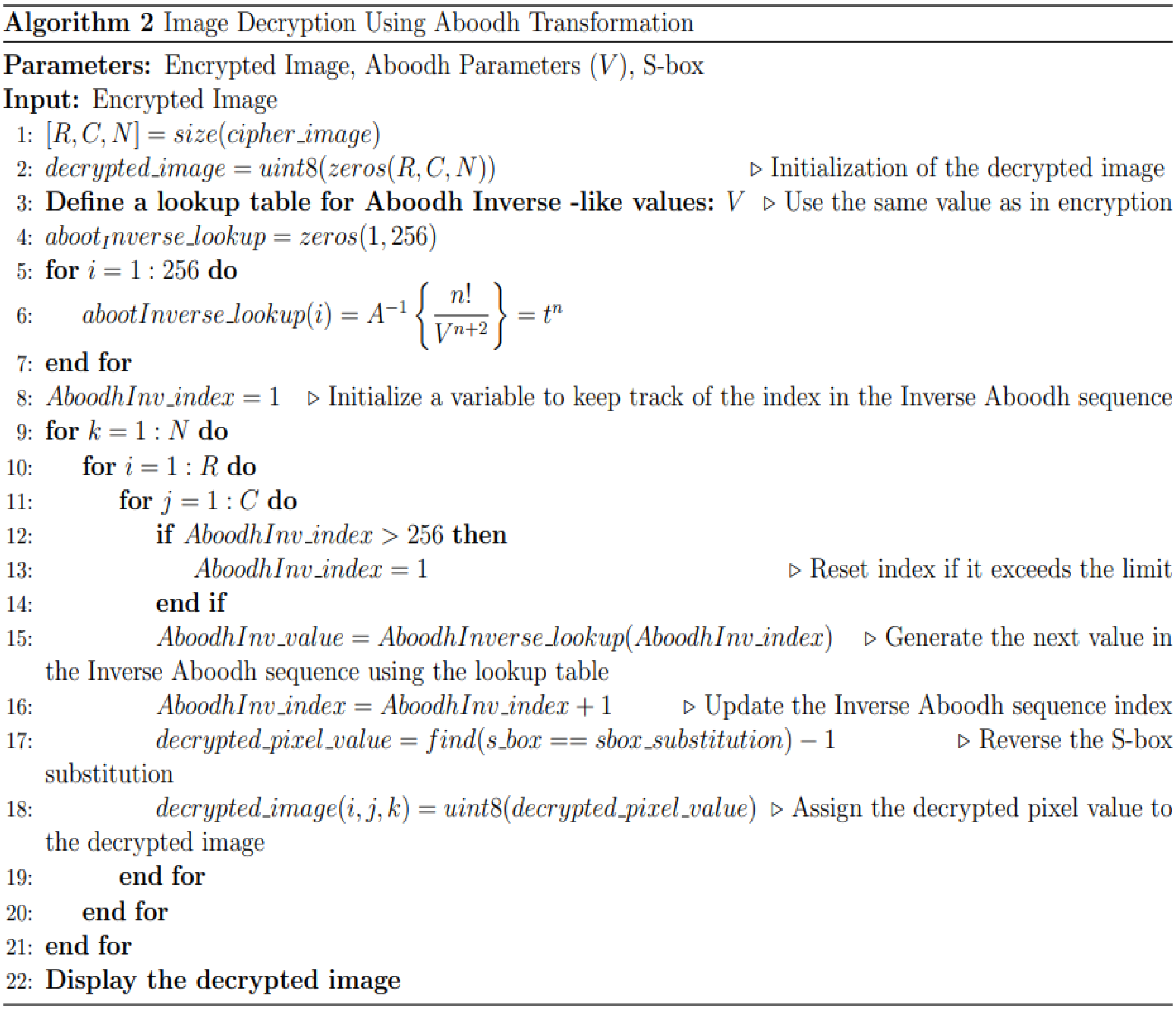
(m) Pepper **(n) Pepper - Encryption** **(o) Pepper - Decryption**

Figure 1. Algorithm Experimental Dataset Images

Decryption Algorithm for Image

A decryption algorithm is a process used to convert encrypted information back into its original, unencrypted form. The decryption algorithm typically uses a key or a password, which must match the encryption key or password used to encrypt the information. The decryption algorithm reverses the encryption process and transforms the cipher image back into the original plain image. The strength of the employed encryption algorithm and the security of the decryption key both affect the security of a decryption algorithm. The decryption algorithm of the proposed cryptosystem is the reverse of the encryption algorithm.

In a closed setting or by using the appropriate asymmetric cryptography mechanism for key distribution, the sender and the receiver may reveal the key parameters used in the encryption process beforehand. After the key has been encrypted, one of the asymmetric cryptography algorithms is used to carry out the decryption process on the receiver's device, sharing the key's value with both the sender and the receiver. The method of the suggested decryption algorithm is explained in Algorithm 2.



Algorithm 2 Image Decryption Using Aboodh Transformation

```
Parameters: Encrypted Image, Aboodh Parameters ($V$), S-box
Input: Encrypted Image
$[R, C, N] = size(cipher\_image)$
$decrypted\_image = uint8(zeros(R, C, N))$    ▷ Initialization of the decrypted image
Define a lookup table for Aboodh Inverse -like values: $V$    ▷ Use the same value as in encryption
$aboot_Inverse\_lookup = zeros(1, 256)$
for $i = 1 : 256$ do
    $abootInverse\_lookup(i) = A^{-1}\left\{\frac{n!}{V^{n+2}}\right\} = t^n$
end for
$AboodhInv\_index = 1$    ▷ Initialize a variable to keep track of the index in the Inverse Aboodh sequence
for $k = 1 : N$ do
    for $i = 1 : R$ do
        for $j = 1 : C$ do
            if $AboodhInv\_index > 256$ then
                $AboodhInv\_index = 1$    ▷ Reset index if it exceeds the limit
            end if
            $AboodhInv\_value = AboodhInverse\_lookup(AboodhInv\_index)$    ▷ Generate the next value in the Inverse Aboodh sequence using the lookup table
            $AboodhInv\_index = AboodhInv\_index + 1$    ▷ Update the Inverse Aboodh sequence index
            $decrypted\_pixel\_value = find(s\_box == sbox\_substitution) - 1$    ▷ Reverse the S-box substitution
            $decrypted\_image(i, j, k) = uint8(decrypted\_pixel\_value)$    ▷ Assign the decrypted pixel value to the decrypted image
        end for
    end for
end for
Display the decrypted image
```

Results and Discussion

Performance Evaluation of Image Cryptosystems

The performance of the proposed image cryptosystem is tested on a personal computer that already has MATLAB 2023 pre-installed on it. These tests are carried out so that the effectiveness of the image cryptosystem may be verified. The five standard pictures included in the dataset of used photos are as follows: an aero plane, a baboon, a boat, a house and a pepper. The most important crucial parameter is the Abooth value, denoted by V, together with the index values. The performance of the recommended technique in both encryption and decryption is seen in Fig. 1.

The effectiveness of an image encryption method relies on two key factors: the duration of encryption sustainability and the algorithm's ability to withstand various types of attacks, including brute force, statistical cryptanalysis, and differential cryptanalysis, among others. The subsequent sections elaborate on these elements to demonstrate the efficacy of the suggested image encryption approach.

Correlation Performance

A correlation attack involves the cryptanalyst's effort to unveil connections between encrypted data and plaintext, seeking patterns or relationships that could reveal the original plaintext or encryption key. One method of statistical analysis pertinent to this is correlation coefficient analysis, which visually illustrates the distribution of neighboring pixels in both original and encrypted images. Typically, plain images exhibit high correlations among neighboring pixels, while encrypted images tend to display fewer connections among adjacent pixels.

In detail, correlation coefficients between each pixel value and its neighboring pixels in a plain image approach a value close to one, whereas in cipher images, they tend to approach zero. When computing these coefficients for plain and encrypted images, pixel selections are randomized. Table 1 showcases the correlation coefficients for plain images alongside their cipher counterparts, revealing cipher image correlation values nearing zero. Additionally, Fig. 2 portrays the correlation distribution for both plain and encrypted images. These findings substantiate the capability of the proposed cryptosystem to resist correlation analysis.

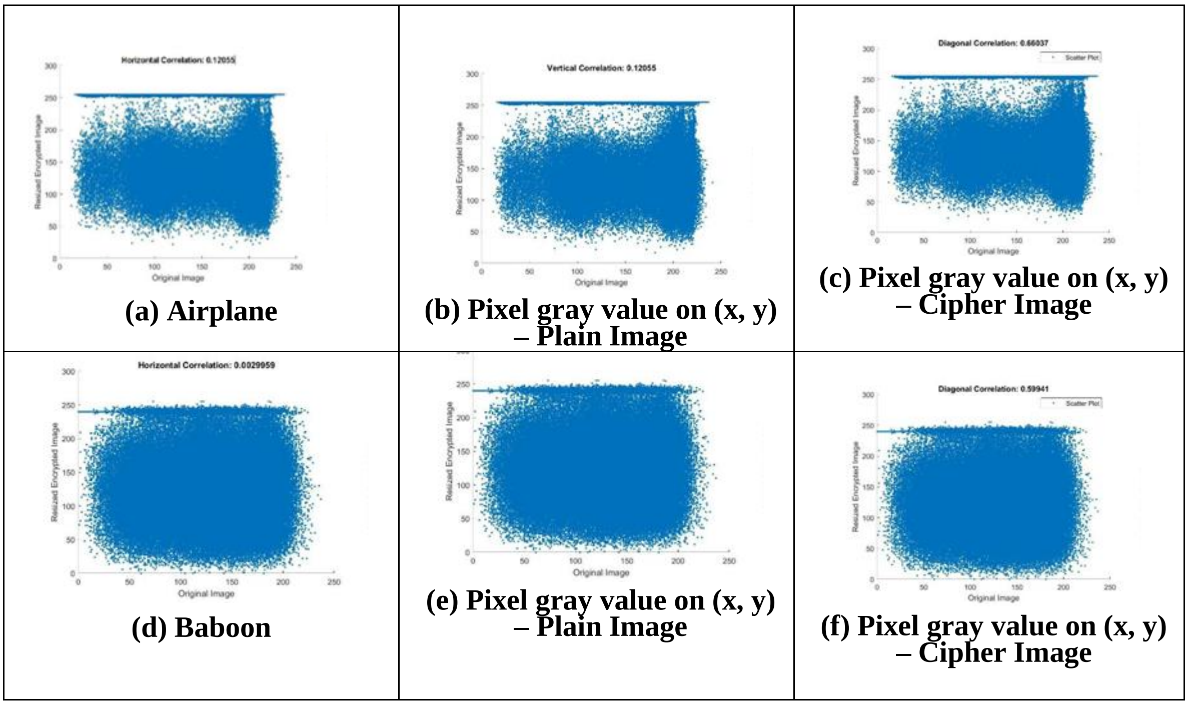
The Eq. 5 used to compute the correlation coefficient is as follows:

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{i=1}^{N}(x_i)\sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{i=1}^{N}(y_i)}{\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{i=1}^{N}(x_i)^2 \sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{i=1}^{N}(y_i)^2} \qquad 5$$

The intensity values of the two adjacent image pixels are shown here as x and y. Fig. 2 displays the correlations that were discovered for both the encrypted and original images. In the original image and then cryptic version, the correlations between pixel boundaries are very strong and very low, respectively. The average correlation coefficients for both plain and encrypted images are summarized in Table 1. The suggested approach performs strong encryption in terms of the degree of correlation between adjacent pixels, proving that it has good confusion and diffusion qualities.

Table 1. Plain and cipher image Correlation Coefficients

	Direction		
Image	**Horizontal**	**Vertical**	**Diagonal**
Airplane	0.1205	0.1205	0.6604
Baboon	0.0301	0.0301	0.5994
Boat	0.1027	0.1027	0.5418
House	0.2033	0.2033	0.6402
Pepper	0.0452	0.0452	0.4911



(a) Airplane

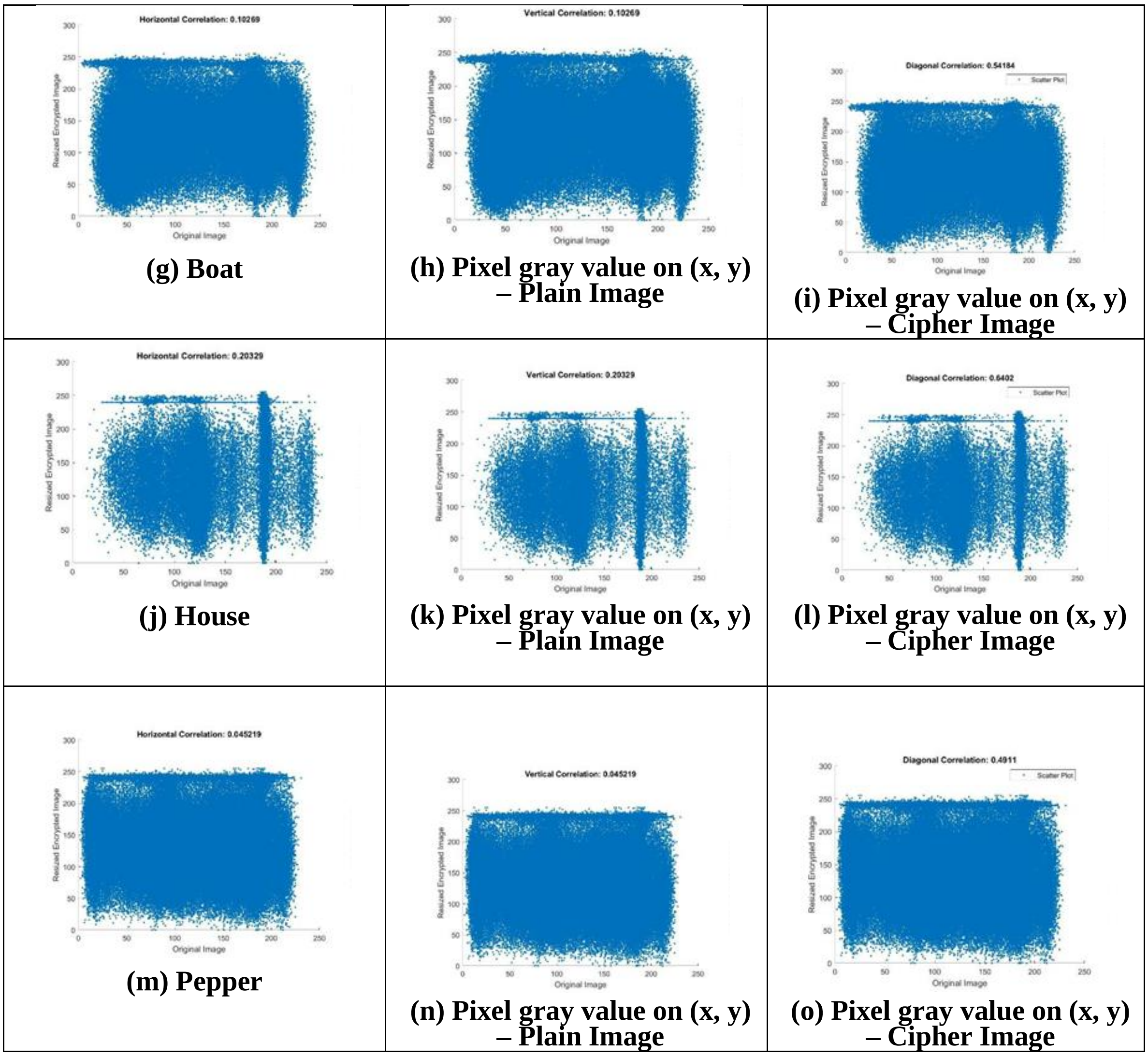
(b) Pixel gray value on (x, y) – Plain Image

(c) Pixel gray value on (x, y) – Cipher Image

(d) Baboon

(e) Pixel gray value on (x, y) – Plain Image

(f) Pixel gray value on (x, y) – Cipher Image



(g) Boat

(h) Pixel gray value on (x, y) – Plain Image

(i) Pixel gray value on (x, y) – Cipher Image

(j) House

(k) Pixel gray value on (x, y) – Plain Image

(l) Pixel gray value on (x, y) – Cipher Image

(m) Pepper

(n) Pixel gray value on (x, y) – Plain Image

(o) Pixel gray value on (x, y) – Cipher Image

Figure 2. Correlation distribution for Plain and Cipher images

Histogram Test

Histogram analysis, a security assessment method, unveils the statistical traits of an encrypted image. During this test, the encrypted image undergoes segmentation into smaller blocks, where the frequency of each intensity level is tallied and depicted as a histogram. The comparison occurs between this histogram of the encrypted image and the anticipated histogram of a random image. A close match indicates that the encryption process introduced adequate randomness, validating the encryption algorithm's functionality. This analysis aids in identifying specific encryption attacks, like substitution attacks, wherein an attacker swaps one pixel value with another in the encrypted image, causing a substantial deviation from the expected histogram of a random image.

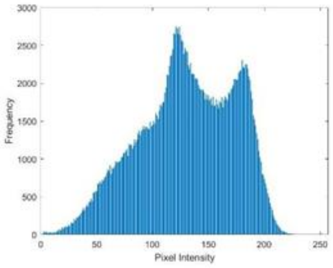
The histogram of a ciphered image showcases the distribution of pixels within the image, plotting pixel count against color intensity levels. Achieving a perfectly ciphered image entails a uniform distribution of pixels across color intensity values. Our proposed approach demonstrates this uniform distribution, eliminating susceptibility to statistical attacks. An effective image cryptosystem should ensure consistent histograms across different ciphered images. In Fig. 3, histograms of plain images are juxtaposed with their respective ciphered counterparts, revealing consistent patterns. The similarity among histograms for ciphered images is quantitatively assessed using variance (Var), denoted in Eq. 6. This variance confirms the likeness among the histograms for the ciphered images

$$Var(T) = \frac{1}{255^2}\sum_{p=0}^{255}\sum_{q=0}^{255}\frac{(t_p-t_q)^2}{2} \qquad 6$$

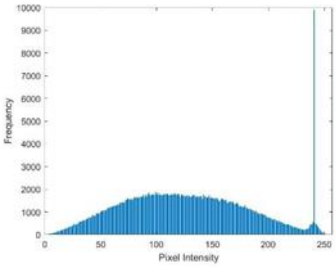
Wheret_p and t_q are pixel numbers whose grey values are p and q, respectively, and $T = t_0, t_1, \dots, t_{255}$ is the sequence of the histogram values. Table 7 displays the histogram variance results for the tested images both before and after the encryption operation. Low numbers show a homogenous distribution in the histograms.

Table 2. Histogram Variance for Plain and Cipher Images

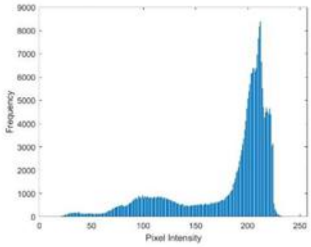
	Variance Value	
Image	Plain	Cipher
Airplane	1942.50	5153.53
Baboon	3105.32	5977.60
Boat	1584.94	5566.84
House	2703.33	4898.93
Pepper	1329.86	5503.22



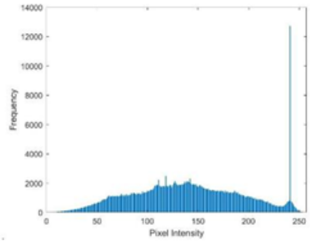
(a) Histogram Airplane -Plain Image



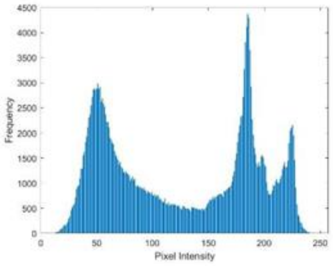
(b) Histogram Airplane - Cipher Image



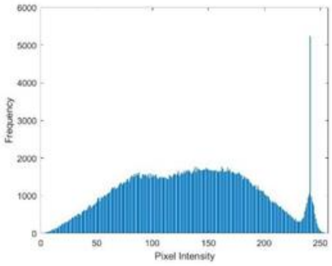
(c) Histogram Baboon -Plain Image



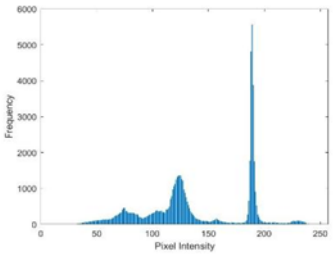
(d) Histogram Baboon -Cipher Image



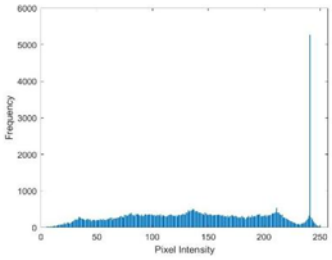
(e) Histogram Boat -Plain Image



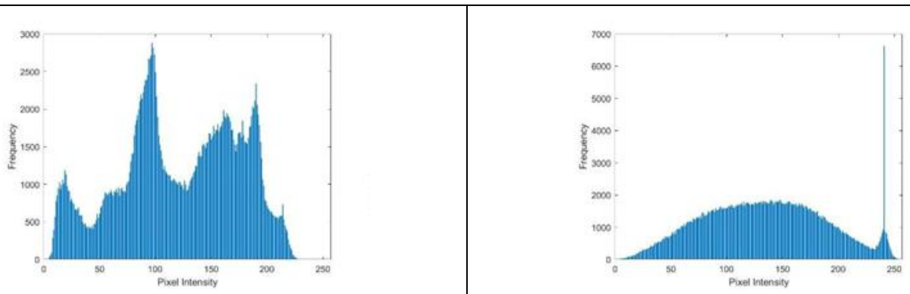
(f) Histogram Boat - Cipher Image



(g) Histogram House -Plain Image



(h) Histogram House -Cipher Image



(i) Histogram Pepper -Plain Image **(j) Histogram Pepper -Cipher Image**

Figure 3. Histogram Analysis

Information Entropy

Information entropy measures the degree of randomness in a particular message. In reality, the entropy of an encrypted image is determined by breaking it up into segments and figuring out the entropy of each one. The probability of each intensity level in a block is calculated, and the entropy is then calculated using this data. This process is done for each block. The encryption algorithm may be operating as intended and the encrypted image may be secure if the entropy of the encrypted image is close to the maximum entropy for a certain image format. The entropy of a perfect grayscale image is eight.

The proposed image cryptosystem's effectiveness is evaluated using the information entropy test on the plain and its analog cipher images. Table–3 displays the entropy results, and the cipher image entropy values are near to 8. The results show that the suggested cryptosystem is entropy resistant.

Table 3. Plain and cipher image Correlation Coefficients

Information Entropy		
Image	Plain	Cipher
Airplane	6.72	7.59
Baboon	7.37	7.65
Boat	7.47	7.73
House	6.47	7.61
Pepper	7.58	7.68

Differential Analyses

Differential analysis is a powerful tool for breaking encryption algorithms, and it has been used to successfully attack many encryption algorithms, including DES and RSA. To defend against differential analysis, encryption algorithms must be designed to resist differential attacks, and they must be thoroughly tested to ensure that they are secure against known types of differential attacks.

Any secure image cryptosystem must have plain image sensitivity, which allows even the smallest changes to the plain image to significantly alter the cipher image. NPCR (Number of Pixels Change Rate) and UACI tests are conducted to evaluate the proposed cryptosystem's plain image sensitivity (Unified Average Changing Intensity) and which are defined by the Eq. 7 and Eq. 8.

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{N} \mathrm{Diff(i)}}{N} \times 100\ \% \qquad 7$$

$$\mathrm{Diff(i)} = \begin{cases} 0 & \text{when } S_1(i) = S_2(i) \\ 1 & \text{when } S_1(i) \neq S_2(i) \end{cases}$$

$$\mathrm{UACI} = \frac{1}{N}\left(\sum_{i=1}^{N} \frac{|S_1(i) - S_2(i)|}{255}\right) \times 100\ \% \qquad 8$$

Where N stands for the complete pixel for the image, and S_1, S_2 are two created cipher images for a single Plain image with minor changes to one of its bits. Table 4 presents the findings, which demonstrate that the suggested cryptosystem is susceptible to minute changes in the plain image.

Table 4. NPCR and UACI Values

Image	UACI	NPCR
Airplane	65.23%	13.91%
Baboon	65.28%	14.16%
Boat	65.31%	15.06%
House	65.21%	13.90%
Pepper	65.36%	16.98 %

Key Space and Key Sensitivity

In the realm of encryption, the terms "key space analysis" and "key sensitivity analysis" refer to methodologies for evaluating the security of an encryption algorithm based on the size of the encryption key and the algorithm's susceptibility to changes in the encryption key. The term "keyspace" encompasses the vast number of keys that could be employed in brute-force attacks and should be sufficiently expansive to render such attempts futile. The Aboodh transformation is unraveled using the primary key parameters v during the encryption and decryption stages of the proposed encryption technique. Assuming that digital devices can perform precise calculations, the key space for the provided cryptosystem is deemed adequate for any cryptographic method

Key sensitivity is an essential attribute of a secure cryptosystem. Even minor alterations to the key should yield significantly different outcomes. To gauge the key sensitivity of the proposed image cryptosystem, the cipher image of Airplane and pepper was repeatedly decrypted by introducing minute adjustments to the key settings. For a quantitative assessment of key sensitivity, an NPCR test was conducted on the decrypted Airplane and pepper image using the real key and on additional encrypted images generated with markedly different initial keys, as illustrated in Fig. 4. The results are presented in Table 5

Table 5. Approximate encrypted pixels different between the two encrypted Images

Experimental Images	Key Sensitivity (%)
Airplane(Fig.4a and Fig.4b)	26.05 %
Baboon(Fig. 5b and Fig. 5f)	26.09 %
Boat(Fig.5c and Fig.5g)	21.27 %
House (Fig.10e and Fig.10f)	21.07 %
Pepper(Fig.4c and Fig.4d)	20.75 %

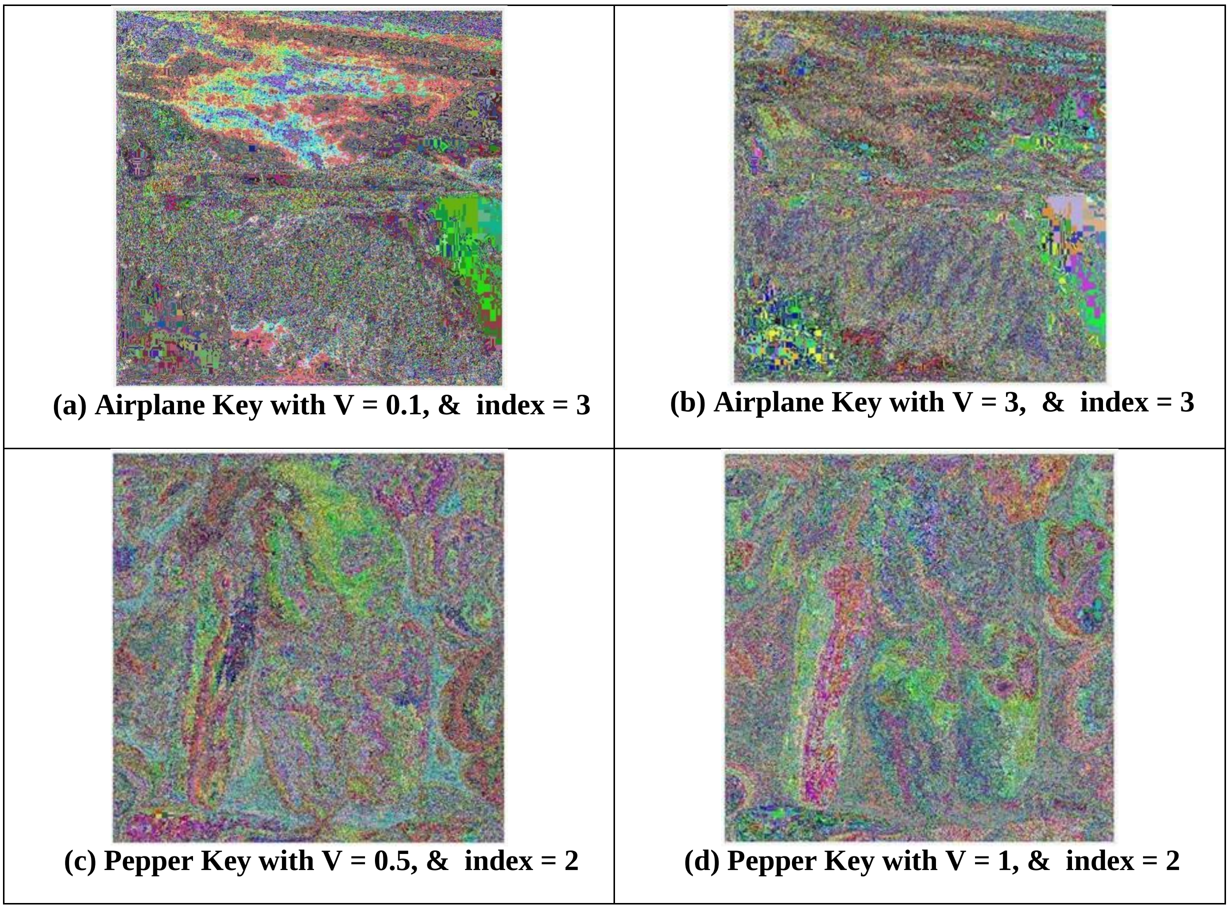
Data Loss Attack

The encrypted data might face risks of loss during transmission through communication channels. Any image encryption system should withstand efforts to trace users. Introducing Gaussian noise blocks into the encrypted image and subsequently trying to decrypt it to retrieve the hidden data would assess the image encryption system's resilience against data loss threats. Fig. 5 displays the outcomes of these data loss attacks, demonstrating the potential successful recovery of the original image from the flawed encryption. To gauge the visual fidelity of restored images from flawed encryption, the Peak Signal-to-Noise Ratio (PSNR), denoted mathematically as an Eq. 9 and Eq. 10, serves as a measure of their visual quality.

$$PSNR(P, D) = 20log_{10}\left(\frac{255}{\sqrt{MSE(P,D)}}\right) \qquad 9$$

$$MSE(P, D) = \frac{1}{x \times y}\sum_{i=1}^{x}\sum_{j=1}^{y}[P(ij) - D(ij)]^2 \qquad 10$$

where D denotes the image that recovered from the flawed image, and $x \times y$ represents a dimension of the plain image P. Table 6 shows the results of the PSNR test for the retrieved image and the plain Airplane, a baboon, a boat, a house and a pepper image. As can be observed from the results shown in Fig. 5 and Table 6, the restored image loses more visual quality as more data is lost in the defective image. Table 7 shows the MSE and PSNR values for plain and decrypted images.



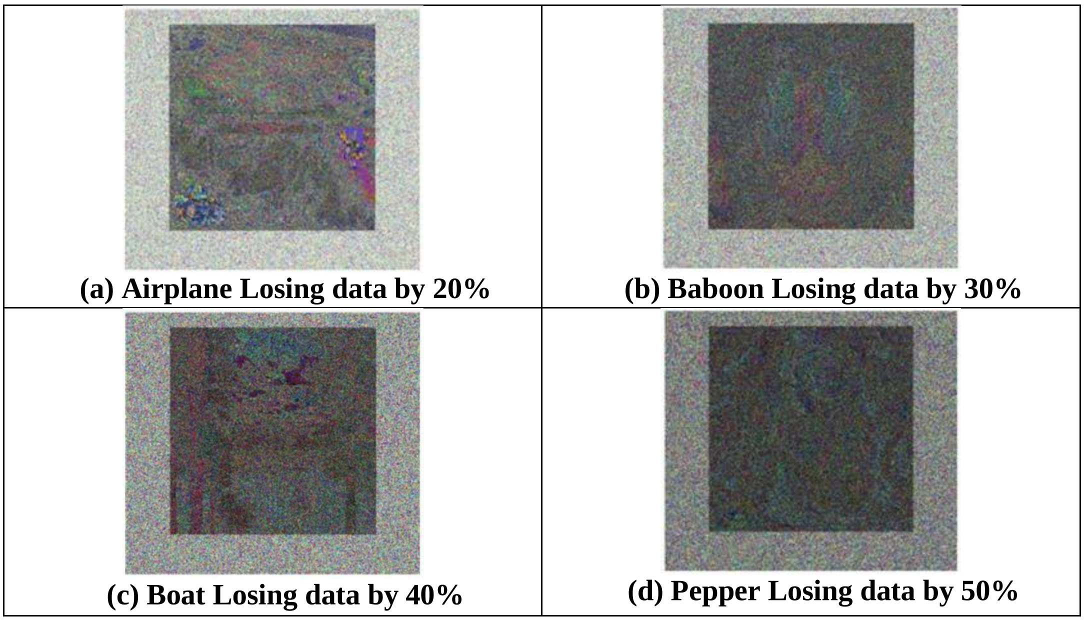
(a) Airplane Key with V = 0.1, & index = 3

(b) Airplane Key with V = 3, & index = 3

(c) Pepper Key with V = 0.5, & index = 2

(d) Pepper Key with V = 1, & index = 2

Figure 4. Decryption effects of cipher images when making small changes in the key parameters.

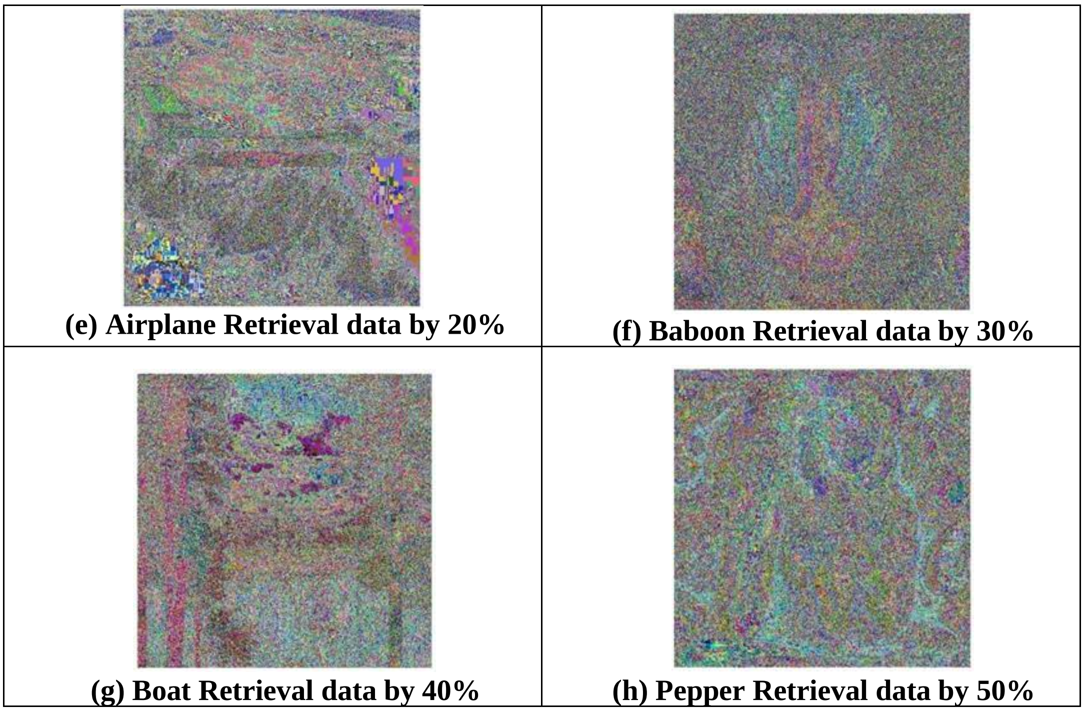


(a) Airplane Losing data by 20%

(b) Baboon Losing data by 30%

(c) Boat Losing data by 40%

(d) Pepper Losing data by 50%



(e) Airplane Retrieval data by 20%

(f) Baboon Retrieval data by 30%

(g) Boat Retrieval data by 40%

(h) Pepper Retrieval data by 50%

Figure 5. Results of data loss attacks, retrieve defectively from the defective cipher image

Table 6. Lossing plain and cipher image MSE and PSNR Details

	Lossing Data Details							
	20%		**30%**		**40%**		**50%**	
Image	**MSE**	**PSNR (dB)**	**MSE**	**PSNR (dB)**	**MSE**	**PSNR (dB)**	**MSE**	**PSNR (dB)**
Airplane	343.95	22.77	514.40	21.02	687.12	19.76	858.79	18.79
Baboon	418.86	21.91	624.60	20.17	826.39	18.96	1033.40	17.99
Boat	405.02	22.06	600.26	20.35	797.30	19.11	989.02	18.18
House	255.09	24.06	380.56	22.33	510.91	21.05	644.24	20.04
Pepper	386.27	22.06	571.67	20.56	763.32	19.30	951.56	18.35

Table 7. MSE and PSNR Value for Plain and decrypted Images

Image	**MSE**	**PSNR (dB)**
Airplane	2714.17	13.80
Baboon	2289.66	14.55
Boat	2672.62	14.01
House	2645.23	13.94
Pepper	2641.76	13.97

Comparative Reliability

Comparative reliability involves assessing various image cryptosystems to determine their dependability and consistency. Table 8 provides a comparison among different image cryptosystems, offering insights into their respective strengths and weaknesses.

The key advantages of the suggested encryption technique are outlined below:

1. Correlation Analysis: Statistics in Table 1 demonstrate the proposed cryptosystem's resilience to correlation analysis, with cipher image correlation coefficients ranging between 0 and 1.

2. Sensitivity to Alterations: Data in Table 5 highlights the proposed cryptosystem's sensitivity to even minor alterations in the plain image.
3. Consistent Histograms: The consistency among cipher image histograms is illustrated in Fig. 3, reinforcing the method's reliability.
4. Histogram Uniformity: Results in Table 2 showcase strong uniformity within cipher image histograms.
5. Entropy Analysis: As indicated in Table 3, the entropy values for cipher images over around 8, indicating the cryptosystem's resilience to entropy analysis.
6. Key Sensitivity: Fig. 4 and Table 7 reveal the high sensitivity of the proposed encryption method to key changes, emphasizing its responsiveness to even minor alterations in initial keys
7. Visual Quality and Data Loss: Results in Fig. 5 and Table 6 demonstrate that as more data is lost from the flawed image, the restored image experiences a greater decline in visual quality.

These highlighted benefits collectively underscore the robustness and effectiveness of the proposed image encryption technique across various analyses and alterations.

Table 8. Comparison of Different Image Cryptosystems

	Comparison		
Image Cryptosystem	**Information Entropy**	**UACI**	**Correlation**
Proposed(references)	7.81	65.30%	0.6604
Khan, and Azam[4]	7.25	64.24%	0.0021
Abd El-Latif, et al[6]	7.79	65.24%	0.0065
Badr, et al [12]	7.69	65.29%	0.0155
Wang, et al [18]	7.23	64.18%	0.0028
Al-Hassani [25].	7.80	65.18%	0.0013

The afore mentioned key points involve comparing the average values of information entropy, NPCR, UACI, and correlation coefficients among encryption systems with the provided average values. This information is utilized to assess the effectiveness of the suggested image cryptosystem, subsequently measuring it against other relevant methods.

Conclusion

Aboodh and its inverse transform, along with the S-Box technique, are used in the suggested cryptographic scheme. The expansion of the hyperbolic cosine function that has been provided is subjected to application of the Aboodh transform. The effectiveness of the suggested technique for encrypting and decrypting the data has been tested using a variety of different pictures. A variety of tests confirmed the suggested algorithm's effectiveness. After investigating the correlation between the plain and chipper images, the results show that there is a substantial association between the two types of images. The sensitivity of the key determined using the Hamming distance. Due of its closeness to 8, the entropy value of information lends credence to the suggested method. Aboodh-based encryption algorithm designed for the image crypto system has been strongly supported by many tests, such as NPCR, UACI, histogram analysis, and PSNR value analysis. In future research, there's an exploration of combining Aboodh and S-box techniques, intending to expand this approach further by integrating DNA coding. The integration of DNA coding alongside Aboodh and S-box methods aims to amplify the complexity of the encryption process. This increased complexity holds the promise of improving secure communication, especially during the transmission of images.

Authors' Declaration

- Conflicts of Interest: None.

- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at University of Technology and Applied Sciences, Oman.

Authors' Contribution Statement

S. R. contributed to the conception, design, data acquisition, analysis, interpretation, drafting of the manuscript, and revising it critically for important intellectual content. R. M. focused on drafting the manuscript, revising it critically, and providing proofreading assistance. S. K. K. participated in data acquisition, analysis, interpretation, and drafting the manuscript. K. R. M. contributed to data acquisition, analysis, and interpretation. N. B. N. was involved in drafting the manuscript, revising it critically, and providing proofreading support.

References

1. Kamrani A, Zenkouar K, Najah S. A new set of image encryption algorithms based on discrete orthogonal moments and Chaos theory. Multimed Tools Appl. 2020 Jul; 79: 20263-79. https://doi.org/10.1007/s11042-020-08879-6.
2. Kang Y, Huang L, He Y, Xiong X, Cai S, Zhang H. On a symmetric image encryption algorithm based on the peculiarity of plaintext DNA coding. Symmetry. 2020 Aug 21; 12(9): 1393. https://doi.org/10.3390/sym12091393.
3. Khan JS, Kayhan SK. Chaos and compressive sensing based novel image encryption scheme. J Inf Secur Appl. 2021 May 1; 58: 102711. https://doi.org/10.1016/j.jisa.2020.102711.
4. Khan M, Azam NA. Right translated AES gray S-boxes. Secur Commun Netw. 2015 Jun; 8(9): 1627-35. https://doi.org/10.1002/sec.1110.
5. Abd El-Latif AA, Abd-El-Atty B, Amin M, Iliyasu AM. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. Sci Rep. 2020 Feb 6; 10(1): 1930. https://doi.org/10.1038/s41598-020-58636-w.
6. El-Latif AA, Abd-El-Atty B, Belazi A, Iliyasu AM. Efficient chaos-based substitution-box and its application to image encryption. Electronics. 2021 Jun 10; 10(12): 1392. https://doi.org/10.3390/electronics10121392.
7. Rajagopal K, Kingni ST, Khalaf AJ, Shekofteh Y, Nazarimehr F. Coexistence of attractors in a simple chaotic oscillator with fractional-order-memristor component: Analysis, FPGA implementation, chaos control and synchronization. Eur Phys J Spec Top. 2019 Oct; 228: 2035-51. https://doi.org/10.1140/epjst/e2019-900001-8.
8. Wen H, Yu S, Lü J. Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos. Entropy. 2019 Mar 5; 21(3): 246. https://doi.org/10.3390/e21030246.
9. Lambić D. S-box design method based on improved one-dimensional discrete chaotic map. J Inf Telecommun. 2018 Apr 3; 2(2): 181-91. https://doi.org/10.1080/24751839.2018.1434723.
10. Özkaynak F, Özer AB. A method for designing strong S-Boxes based on chaotic Lorenz system. Phys Lett A. 2010 Aug 9; 374(36): 3733-8. https://doi.org/10.1016/j.physleta.2010.07.019.
11. Wang Y, Wong KW, Li C, Li Y. A novel method to design S-box based on chaotic map and genetic algorithm. Phys Lett A. 2012 Jan 30; 376 (6-7): 827-33. https://doi.org/10.1016/j.physleta.2012.01.009.
12. Badr AM, Fourati LC, Ayed S. A Novel System for Confidential Medical Data Storage Using Chaskey Encryption and Blockchain Technology. Baghdad Sci J. 2023 Dec. 5; 20(6(Suppl.): 2651. http://dx.doi.org/10.21123/bsj.2023.9203
13. Hamza YA, Tewfiq NE, Ahmed MQ. An Enhanced Approach of Image Steganographic Using Discrete Shearlet Transform and Secret Sharing. Baghdad Sci J. 2022 Feb. 1; 19(1): 0197. https://doi.org/10.21123/bsj.2022.19.1.0197.
14. Al-Bahrani EA, Kadhum RN. A new cipher based on Feistel structure and chaotic maps. Baghdad Sci J. 2019 Jan 2; 16(1): 270-80. https://doi.org/10.21123/bsj.2019.16.1(Suppl.).0270.
15. Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans Circuits Syst. 2001 Feb; 148(2): 163-9. https://doi.org/10.1109/81.904880.
16. Özkaynak F. Construction of robust substitution boxes based on chaotic systems. Neural Comput & Applic.

2019 Aug; 31(8): 3317-26. https://doi.org/10.1007/s00521-017-3287-y.

17. Özkaynak F, Çelik V, Özer AB. A new S-box construction method based on the fractional-order chaotic Chen system. Signal Image Video P. 2017 May; 11: 659-64. https://doi.org/10.1007/s11760-016-1007-1.
18. Wang Y, Zhang Z, Zhang LY, Feng J, Gao J, Lei P. A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. Inf. Sci. 2020 Jun 1; 523: 152-66. https://doi.org/10.1016/j.ins.2020.03.025.
19. Yousaf MA, Alolaiyan H, Ahmad M, Dilbar M, Razaq A. Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes. IEEE Access. 2020 Feb 24; 8: 39781-92. https://doi.org/10.1109/ACCESS.2020.2975880.
20. Zhang T, Chen CP, Chen L, Xu X, Hu B. Design of highly nonlinear substitution boxes based on I-Ching operators. IEEE Trans. Cybern. 2018 Jul 23; 48(12): 3349-58. https://doi.org/10.1109/TCYB.2018.2846186.
21. Gautam A, Gaba GS, Miglani R, Pasricha R. Application of chaotic functions for construction of strong substitution boxes. Indian J Sci Technol. 2015 Oct 23; 8(28): 1-5. https://doi.org/10.17485/ijst/2015/v8i28/71759.
22. Haider MI, Ali A, Shah D, Shah T. Block cipher's nonlinear component design by elliptic curves: an image encryption application. Multimed Tools Appl. 2021 Jan; 80: 4693-718. https://doi.org/10.1007/s11042-020-09892-5.
23. Hussain I, Azam NA, Shah T. Stego optical encryption based on chaotic S-box transformation. Opt Laser Technol. 2014 Sep 1; 61: 50-6. https://doi.org/10.1016/j.optlastec.2014.01.018.
24. Siddiqui N, Naseer A, Ehatisham-ul-Haq M. A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve. Wirel Pers Commun. 2021 Feb; 116(4): 3015-30. https://doi.org/10.1007/s11277-020-07832-y.
25. Al-Hassani MD. A Novel Technique for Secure Data Cryptosystem Based on Chaotic Key Image Generation. Baghdad Sci J. 2022 Aug. 1; 19(4): 0905. https://doi.org/10.21123/bsj.2022.19.4.0905
26. Azam NA, Ullah I, Hayat U. A fast and secure public-key image encryption scheme based on Mordell elliptic curves. Opt Lasers Eng. 2021 Feb 1; 137: 106371. https://doi.org/10.1016/j.optlaseng.2020.106371.
27. Meranza-Castillón MO, Murillo-Escobar MA, López-Gutiérrez RM, Cruz-Hernández C. Pseudorandom number generator based on enhanced Hénon map and its implementation. Int J Electron Commun. 2019 Jul 1; 107: 239-51. https://doi.org/10.1016/j.aeue.2019.05.028.
28. Khudair ET, Naser EF, Mazher AN. Comparison between RSA and CAST-128 with Adaptive Key for Video Frames Encryption with Highest Average Entropy. Baghdad Sci J. 2022 Dec. 1; 19(6):1378. https://doi.org/10.21123/bsj.2022.6398
29. Mohan KR, Nagaram NB, Murugesan R, Rasappan S. A Cryptographic Technique Using Conformal Mapping. In Recent Trends in Computational Intelligence and Its Application.2023 Jun 15; (pp. 519-523). CRC Press. https://doi.org/10.1201/9781003388913-69.
30. Nagaram NB, Mohan KR, Kumaravel SK, Rasappan S. Secret Sharing of Information using First Order ODE and Variable Separable Method. In Recent Trends in Computational Intelligence and Its Application .2023 Jun; 15 (pp. 515-518). CRC Press. https://doi.org/10.1201/9781003388913-68.
31. Murillo-Escobar MA, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez RM. Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller. Microprocess. Microsyst. 2016 Sep 1; 45: 297-309. https://doi.org/10.1016/j.micpro.2016.06.004
32. Wang X, Feng L, Zhao H. Fast image encryption algorithm based on parallel computing system. Inf. Sci.. 2019 Jun 1; 486: 340-58, https://doi.org/10.1016/j.ins.2019.02.049.
33. Diaconu AV. Circular inter–intra pixels bit-level permutation and chaos-based image encryption. Inf. Sci.. 2016 Aug 10; 355: 314-27. https://doi.org/10.1016/j.ins.2015.10.027.
34. Abd El-Latif AA, Ramadoss J, Abd-El-Atty B, Khalifa HS, Nazarimehr F. A Novel Chaos-Based Cryptography Algorithm and Its Performance Analysis. Mathematics. 2022 Jul 1; 10(14): 2434. https://doi.org/10.3390/math10142434.
35. Gan ZH, Chai XL, Han DJ, Chen YR. A chaotic image encryption algorithm based on 3-D bit-plane permutation. Neural Computing and Applications. 2019 Nov; 31: 7111-30. https://doi.org/10.1007/s00521-018-3541-y.

تحليل كفاءة طريقة جديدة لتشفير الصور بناء على تحويلات أبوده

سوريش راسابان[1]، ريجان موروجيسان[2]، ساتيش كومار كومارافيل[2]، كالا راجا موهان[2]، ناجاديفي بالا ناجارام[2]

[1]قسم الرياضيات، الجامعة التقنية والعلوم التطبيقية، عبري، سلطنة عمان.
[2]قسم الرياضيات، معهد فيل تيك رانجاراجان د. ساجونثالا للبحث والتطوير للعلوم والتكنولوجيا، أفادي، تشيناي – 600062، تاميل نادو، الهند.

الخلاصة

الهدف من هذا البحث هو تطوير طريقة تشفير فريدة من نوعها تستخدم طريقة Aboodh وتحويلها العكسي مع طريقة S-Box.تشير نتائج التقييمات إلى أن هذا العمل مناسب للاستخدام في تطبيقات التشفير الآمنة، ويوفر أدلة فيما يتعلق ببناء نظام تشفير للصور بناءً على السلوكيات المعقدة التي يوضحها. بعد تطبيق المنهجيات التي تم تقديمها لتصوير البيانات المأخوذة من مواقف الحياة الواقعية، تم تقييم النتائج باستخدام مجموعة واسعة من المعايير الإحصائية ومعايير الأداء. نتائج هذا التحقيق تؤدي إلى تحسين موثوقية نظام التشفير.

الكلمات المفتاحية: تحول عبود، التشفير، فك التشفير، التشفير، طريقة S-Box.