**Image** **Encryption System**

# ABSTRACT

The implementation of this project is to create a combined pseudo-random sequence generator based on neural networks and chaotic random variable colour images, based on a chaotic encryption algorithm for secure image transmission and storage. The generator that controls the operation of the encryption algorithm: the arrangement of pixel positions, the use of random colour images of the AES algorithm to achieve encryption, create algorithms, and neural networks, by dynamically updating control parameters and numbers to increase the randomness of the generated chaotic sequence by using simulation MATLAB for getting output . The iteration of the chaotic function in the neural network. Various tests, including autocorrelation, 0/1 balance. The experimental results are presented in the form of pixel correlation coefficient and security analysis to prove the security and effectiveness of the proposed chaos-based ANN encryption**.**

Table of Contents

**CHAPTER TITLE PAGES**

[ABSTRACT vii](#_Toc75620880)

[CHAPTER 1 12](#_Toc75620881)

[INTRODUCATION 12](#_Toc75620882)

[1.1 Research Background 12](#_Toc75620883)

[1.2 Objective 14](#_Toc75620884)

[1.3 Problem Statement 14](#_Toc75620885)

[1.4 Scope of work 15](#_Toc75620886)

[1.5 Limitations 16](#_Toc75620887)

[CHAPTER 2 17](#_Toc75620888)

[LITERATURE REVIEW 17](#_Toc75620889)

[2.1 Literature Review 17](#_Toc75620890)

[2.2 Principles of Cryptography 20](#_Toc75620891)

[2.3 Cryptography Phases 20](#_Toc75620892)

[2.4 Types of Cryptography algorithms 21](#_Toc75620893)

[2.4.1 Secret Key Cryptography (SKC) or Symmetric Encryption 21](#_Toc75620894)

[2.4.2 Public Key Cryptography (PKC) or Asymmetric Encryption 22](#_Toc75620895)

[2.5 Cryptography Properties 23](#_Toc75620896)

[2.6 Image Security 24](#_Toc75620897)

[2.6.1 Image Cryptography and Image Steganography 25](#_Toc75620898)

[2.6.2 Randomness 26](#_Toc75620899)

[2.6.3 Size of key 27](#_Toc75620900)

[CHAPTER 3 28](#_Toc75620901)

[RESEARCH METHODOLOGY 28](#_Toc75620902)

[3.1 Introduction 28](#_Toc75620903)

[3.2 Methodology and the Proposed Work 29](#_Toc75620904)

[3.2.1 Algorithm for the Decryption Phase 35](#_Toc75620905)

[3.3 Measurements used to evaluate the proposed algorithm 36](#_Toc75620906)

[3.3.1 Image Histogram 36](#_Toc75620907)

[3.3.2 Peak Signal to Noise Ratio (PSNR) 37](#_Toc75620908)

[CHAPTER 4 38](#_Toc75620909)

[RESULT AND DISCUSSION 38](#_Toc75620910)

[4.1 Implementation 38](#_Toc75620911)

[4.2 System specification used 39](#_Toc75620912)

[4.3 The Expected results 39](#_Toc75620913)

[4.3.1 The Result of the Proposed Experiment 42](#_Toc75620914)

[4.3.2 AES Result 44](#_Toc75620915)

[4.3.3 DES result 45](#_Toc75620916)

[4.4 Comparison among Technique 45](#_Toc75620917)

[4.4.1 SNR dB 45](#_Toc75620918)

[4.4.2 PSNR dB 46](#_Toc75620919)

[4.4.3 NMAE 46](#_Toc75620920)

[4.5 Security Analysis and discussion 47](#_Toc75620921)

[4.5.1 Experimental Results and Security Analysis 48](#_Toc75620922)

[4.6 Robustness and level of security 49](#_Toc75620923)

[4.6.1 Robustness 49](#_Toc75620924)

[4.6.2 Security image 49](#_Toc75620925)

[CHAPTER 5 50](#_Toc75620926)

[CONCLUSION 50](#_Toc75620927)

[5.1 Introduction 50](#_Toc75620928)

[References 52](#_Toc75620929)

**LIST OF TABLES**

**TABLE NO. TITLE PAGE**

[Table ‎0‑1: Images used in experiments 42](#_Toc75621661)

[Table ‎0‑2: Proposed technique result. 45](#_Toc75621662)

[Table ‎0‑3: Using two different keys on the Baboon image. 46](#_Toc75621663)

[Table ‎0‑4: Number of blocks in secret key. 46](#_Toc75621664)

[Table ‎0‑5: Using two different keys on the Lena image. 46](#_Toc75621665)

[Table ‎0‑6: Using two different keys on the Balloon image. 47](#_Toc75621666)

[Table ‎0‑7: AES result. 47](#_Toc75621667)

[Table ‎0‑8: DES Result. 48](#_Toc75621668)

[Table ‎0‑9: PSNR in Proposed, AES and DES. 48](#_Toc75621669)

[Table ‎0‑10: PSNR in Proposed, AES and DES. 49](#_Toc75621670)

[Table ‎0‑11: NMAE in Proposed, AES and DES. 49](#_Toc75621671)

[Table ‎0‑12: Sizes of images and secret keys. 50](#_Toc75621672)

[Table ‎0‑13: Comparison results between Proposed and AES with different sizes images 50](#_Toc75621673)

**LIST OF FIGURES**

**FIGURE NO. TITLE PAGE**

Figure ‎0.1: the basic structure of the cryptographic system 22

Figure ‎0.2: The process of symmetric encryption (Web Service Security, 2005). 24

Figure ‎0.3: the process of asymmetric encryption (Web Service Security, 2005). 25

Figure ‎0.4: Cryptography Properties. 26

Figure ‎0.5: Pixel of RGB. 27

Figure ‎0.1: Diagram of the proposed algorithm. 31

Figure ‎0.2: The architecture and the methodology of the proposed encryption phase. 33

Figure ‎0.3: Histogram Red Green Blue. 39

Figure ‎0.1: Lena image histogram (Original & Encrypted). 42

Figure ‎0.2: Baboon image histogram (Original & Encrypted). 42

Figure ‎0.3: Pepper image histogram (Original & Encrypted). 43

Figure ‎0.4: Balloon image histogram (Original & Encrypted). 43

Figure ‎0.5: Decrypted Lena image using wrong key. 51

# 

INTRODUCATION

## Research Background

Due to the advancement of network and multimedia coding technology, multimedia data such as pictures are often stored and transmitted via the Internet and are vulnerable to malicious use. Therefore, image security and encryption has become a well-researched area to ensure privacy and prevent unauthorized access to digital content. Traditional symmetric encryption, such as Advanced Encryption Standard (AES) , is designed with good confusion and propagation characteristics. However, standard encryption methods such as AES do not seem to be suitable for encrypting data such as images. Since 1990, chaotic systems have attracted great interest in the field of cryptography due to their ideal characteristics such as high sensitivity to conditions. Initials, periodicity, and pseudo-randomness. Chaos systems also show great potential for protecting information, especially when encrypting images. More recently, researchers have shown interest in combining neural networks and chaos to develop and enhance encryption algorithms. The authors in trained the Chaos Neural Network to replace the chaotic generator in the encryption algorithm. In the chaotic map is used as a transfer function for each neuron. They then proposed to use this generator in a stream encryption algorithm where the image is viewed as a one-dimensional array and each bit is encrypted with a chaotic binary output. In the bias and weights of the neural network are adjusted by a chaotic sequence, which would make the output of the neural network very random. The output of the neural network is used to AES encrypt images. , this encryption method uses simple operations like the XOR bit, which makes the proposed mechanism easy to break. The encryption time and the computation processing are also quite high in this case.

Theoretically, chaos generator based on a neural network is proposed. Use the three-dimensional chaotic one-dimensional map to trigger neural network parameters, such as weights, discrimination, and control parameters. The neurons in the neural network are designated by PWLCM as their transfer function. The neural network uses 64 bits (8 8-bit inputs) as the key for the first cycle of its operation and generates a random sequence throughout the cycle. After the entire network cycle, the control parameters for each layer are updated to the same level as the release, keeping the control parameters close to 0.5 (with excellent optimal behaviour). The production process showed a good random structure, as shown by the test. The encryption method is used by the XOR sequence generated by the small picture. After the complete four-layer neural network loop, there is only one element in the output layer. We believe that improvements can be made to reduce congestion on the computer. In addition, the encryption method used by XOR consists only of chaotic fragments of pixelated images that are less secure.

The cryptographic system used to protect data relies on the existence of a large solution space to prevent attacks. In fact, when designing a cryptographic system, the important point is that the underlying algorithm simply uses all possible possibilities of the algorithm to encrypt the target data to prevent attempts to crack it with so-called brute force attacks (Li and, 2002b; Shakir, 1997). In almost all cryptographic algorithms, there are two classic data encryption methods that can be used alone or in combination. Replacement involves systematically replacing bytes in the data with encrypted bytes according to a specific algorithm. Since substitution is relatively easy to automate in mechanical and electronic aspects, it is often used in government and commercial cryptographic systems. It is a kind of transposition, in which the relative order of the bytes constituting the data changes according to r. This is easy to automate, although the advent of microprocessors has led to their incorporation into several modern cryptographic systems, such as the Encrypted Data Standard (DES) (Robert and Matthews, 1993).

## Objective

An unconventional image encryption system is proposed, which uses a large key to protect images containing confidential information. This method greatly increases the value of the image encryption method by using a smart algorithm, making it difficult to be attacked. Can provide a way for image protection and privacy. The contribution of the proposed method is the use of a secret key. This key is divided into multiple blocks. In these blocks, take a row from each cell of the block. This long key ring makes the encryption secure and difficult to crack. This article uses statistical analysis and key sensitivity analysis to evaluate the security of the proposed encryption algorithm.

The objective of this research are:

1. Determining the representation scheme.
2. Determining the parameters and variables for controlling the algorithm.
3. To determine how to calculate the results and criteria for terminating a run.

## Problem Statement

The Digital images are deliberated to be one of the most widely used media in various information networks. Most of these images usually contain highly confidential information. Attackers always try to steal, damage or use these personal photos in various ways to blackmail the owners of these photos. In addition, in recent years, the security of digital images has attracted much attention. This is needed with the rapid development of the Internet and the widespread use of multimedia technology, people can easily share digital multimedia data with others through the Internet, thus providing a reliable method to protect these images from various types of intruders. Encryption Standard, AES-Advanced Encryption Standard are designed to protect text data, but may not be suitable for multimedia. Direct image encryption using traditional cryptographic systems is impossible. It is suitable for two reasons:

(a) The image encryption time is longer because it is larger than the text,

(b) The decrypted text must match the original text, but this is not necessary for the image.

The decoded image can Accepted by the human perception system (Sivakumar, Venkatesan, 2014). Encryption algorithms used currently, such as AES, DES, 3DES...etc. The replacement and transposition process is performed in a conventional method, but not all pixels are covered. In addition, the private key used is not enough. Randomness (Chen et al., 2004). Although many encryption systems have been sophisticated, there are still some problems, such as the length of the pixel so that a clue used, which is an important factor. The main problem with many existing encryption systems is the size of the key used in the encryption process. The key used is 64-bit or 128-bit, which is not enough to ensure the security of the image, so the key plays an important role in achieving the highest level of security.

This work proposes a solution that plans a model (Proposed Method) that uses a large, well-protected random generalization key of at least 2048 bits. The use of the proposed algorithm aims to significantly improve the encrypted image and ensure a high level of protection. .

## Scope of work

In this work, colour samples are used to apply the algorithm by using ANN specialty. Because this method is giving the accurate result with different attempts. These images are only used for bitmaps. The proposed method aims to provide high-speed, high-complexity, large key size and random encryption methods to improve performance and reduce encryption time. C# tools are used for implementation. On the other hand, PC is used in the evaluation process.

## Limitations

During the development and implementation of the proposed method, there were some problems affecting the work

* The first limitation is that only the image is encrypted,
* The image must be in BMP format.

# 

# LITERATURE REVIEW

## Literature Review

Digital images are the most common way of exchanging data between people, in most cases such as sharing an image by using social media, these images contain personal data. Many security researchers put more effort into introducing new, unconventional methods to safely protect these images. Research has been proposed in the field of methods of encrypting and decrypting images. The use of image encryption technology has expanded and has become an important issue for protecting the confidentiality, integrity, and authenticity of images. Various methods are proposed from time to time. It's time to encrypt your pictures to improve security. When using image encryption technology, the pixels in the image are merged, and the correlation between the pixels is reduced, resulting in a reduction in the correlation between the pixels and the encrypted image.

Satish et al. (2011) proposed a new image encryption method based on integrated pixel coding plus diffusion [IISPD]. The proposed algorithm takes advantage of the completely chaotic characteristics of the logic diagram and reduces the time complexity. His research defined how to calculate the arrangement direction of rows and columns by XOR in the adjacent pixel values ​​in the original image bit by bit. Security analysis and experimental analysis show that this method is very sensitive to initial conditions, larger key space and higher encryption.

When comparing this research with [IISPD], the next point is the warning method, because for the [IISPD] method, the encryption method relies on performing a semi-traditional obfuscated XOR operation to encode adjacent pixels row by row and column by column. Use two keys: KX for rows and KY for columns. The encrypted image is obtained in this way because in the proposed method, it uses a series of XOR replacements based on unconventional transposition operations, which results in a change in the order of pixels using a large key.

Measures the [IISPD] technique indicates a correlation ratio of cipher image (-0.0070493) at any picture, at the same time as the ratio indicates (0.079) .these indicates that the cost of the correlation ratio of the cipher picture is higher with inside the proposed technique this means that that the important thing sensitivity is higher in the proposed technique.

Chaumon ​et al. (2013) proposed a method based on the color change algorithm after the quantization step. This process protects the color information in the image by embedding the color information in the image into the corresponding grayscale image. Reordering creates a grayscale image, and a data hiding algorithm can be used to embed the palette in the grayscale image. The structure of the method is shown in the figure. You use the luminance image to quantify the original color image, select a number, and then use the color rearrangement algorithm to get a modified palette and an index image close to the luminance image. The last step is to embed the palette (message) in the index picture (cover). Changing the colour order in these methods depends on the colours in the original image being quantized and converted to appropriate grey values ​​using colour indexes. After that, the generated colours are rearranged in the pattern.

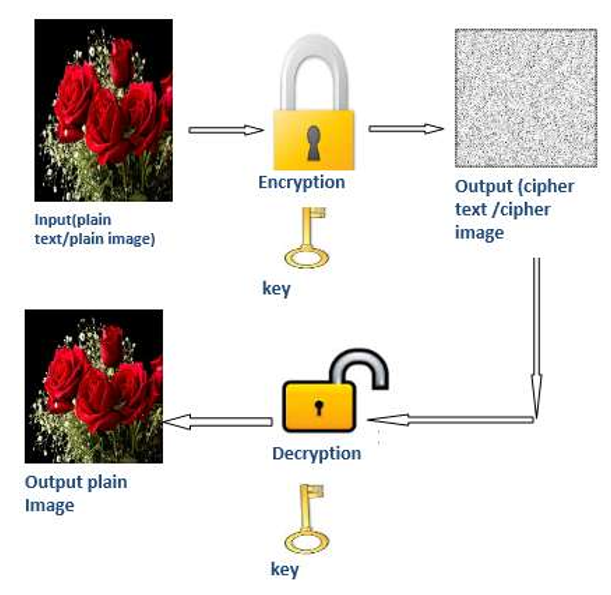
In other words, compared to the method proposed in this study, this method relies on encrypted colours, not data. When viewing the measurement (PSNR) of different images (256 colours each), the current Lena image size value is 315 × 230 PSNR 38.63 DB, and the recommended value is 7.05, the baboon image 256 × 256 is 33.31 inches, and the baboon image is 33.31 inches. The rate is 491 dB, and the Pepper image is 256 × 256 PSNR 36. It is recommended to use 34 and 026 DB. These values ​​indicate that the proposed method is more effective because it includes data and color encryption.

Yun-peng et al., (2009) studies centered at the mixture of photo encryption algorithms like chaotic encryption, DES encryption, etc. In their set of rules, for making the pseudo-random series, logistic chaos the sequencer changed into used; it includes at the RGB with this series to the photo chaotically, after which makes double-time encryptions with development DES. This set of rules had excessive protection and the encryption speed.

## Principles of Cryptography

Cryptography is the science of studying how to protect privacy. There are many ways to hide stored or transmitted information. In addition, cryptography involves encoding images and messages in the form of encryption (an encryption method) and then restoring them to their original form. (Decryption process) In other words, encryption is the process of converting readable information into unreadable or encrypted data (Boneh et al., 2004). In recent research, cryptography is regarded as the mapping field of mathematics and computer science, closely related to information theory, computer security, and engineering research (Bibhudendra et al., 2007). The following figure (2.1) shows the basic structure of the cryptographic system.

Figure ‎0.1: the basic structure of the cryptographic system



## Cryptography Phases

Encryption levels the encryption system usually consists of two levels: the encryption level that converts the original secret data into encrypted data, and the encryption level that converts the encrypted data into the original secret data. The key used in the encryption system represents the strength of the encryption algorithm. These keys must be sufficiently complex and large enough accomplish high security of confidential data. In addition, the implementation of replacement and transposition operations is so complicated that it becomes increasingly difficult to prevent attackers from cracking encrypted data. This process should eliminate the main problem of the current encryption system, that is, the key used is not large enough, and the randomness of the key is low (Lindner and Piker, 2011).

## Types of Cryptography algorithms

The cryptography algorithms can be categorized into three categories based on the number of keys that are employed for encryption and decryption. The three types of cryptography algorithms are presented in the next sections.

### Secret Key Cryptography (SKC) or Symmetric Encryption

Symmetric encryption is the primogenital and most famous method. In this system, the sender and receiver both use the same techniques. This method is also called key encryption (SKC) because a single key is used for encryption and decryption to identify random colour images. So an image can be a number, a word, or just a random sequence of letters, which is applied to the original data to change the content in some way.

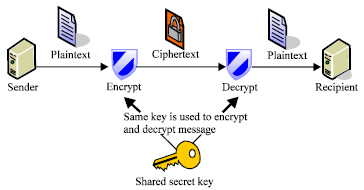
Therefore, all data can communicate as long as both the sender and the recipient have the secret key. Using this key, encrypt and decode all data. Cryptography algorithms such as (DES, 3DES, AES, and RC4) are examples of this kind (Delfs and Knebl, 2007). Figure 1 illustrates the processes of the system (2.2).

Figure ‎0.2: The process of symmetric encryption (Web Service Security, 2005).

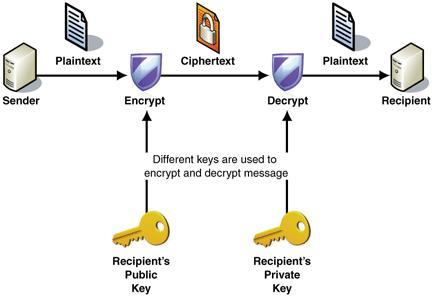
Secret key encryption schemes are usually divided into stream ciphers or block ciphers. The stream cipher processes one bit (byte or computer word) at a time and implements some kind of backtracking mechanism so that the key keeps changing. The block cipher is so named because the scheme uses the same key in each data block to encrypt one data block at a time. If the same key is used in the block cipher, usually the same plaintext block is always encrypted with the same cipher text, and the same plaintext is encrypted with different codes. Due to identify any colour image determine the size of the image although the same plaintext will encrypt to the different cipher text in a stream cipher.

### Public Key Cryptography (PKC) or Asymmetric Encryption

Asymmetric encryption uses two associated keys, one key pair

* A public key that can be used by anyone who wants to send you a message.
* The second key is the private key. It is confidential, so only one person will know. Messages encrypted with a public key (text, binary file, or document) can only be decrypted using the same algorithm, but with the corresponding private key. This implies you don't have to be concerned. About transferring the public key over the Internet (the key essential be public). Figure (2.3) shows the process of asymmetric encryption and asymmetric decryption (Web Service Security, 2005).

Figure ‎0.3: the process of asymmetric encryption (Web Service Security, 2005).



In asymmetric cryptography (also known as public-key cryptography), the sender uses one key to encrypt data, and the receiver uses another key to decrypt the cipher text. The encryption key and its corresponding decryption key are usually called a public key/private key pair. However, asymmetric encryption is leisurelier than asymmetric encryption. Encrypting and decrypting message content requires more computing power. Asymmetric encryption algorithms include (RSA, Daffier Hellman, digital signature, ECDSA, and XTR).

## Cryptography Properties

Cryptography provides many security features to ensure data secrecy and data immutability. Due to the huge security advantages of cryptography, it is widely used today. The most ideal feature of any image cryptography is to maximize the strength of the key. In order to avoid hacker attacks and protect it from being discovered by unauthorized persons, the following figure (2.4) shows the characteristics of cryptography. The following sections show the different uses of cryptography (the delayed fourth edition).

Figure ‎0.4: Cryptography Properties.

Confidentiality

Authentication

Integrity

## Image Security

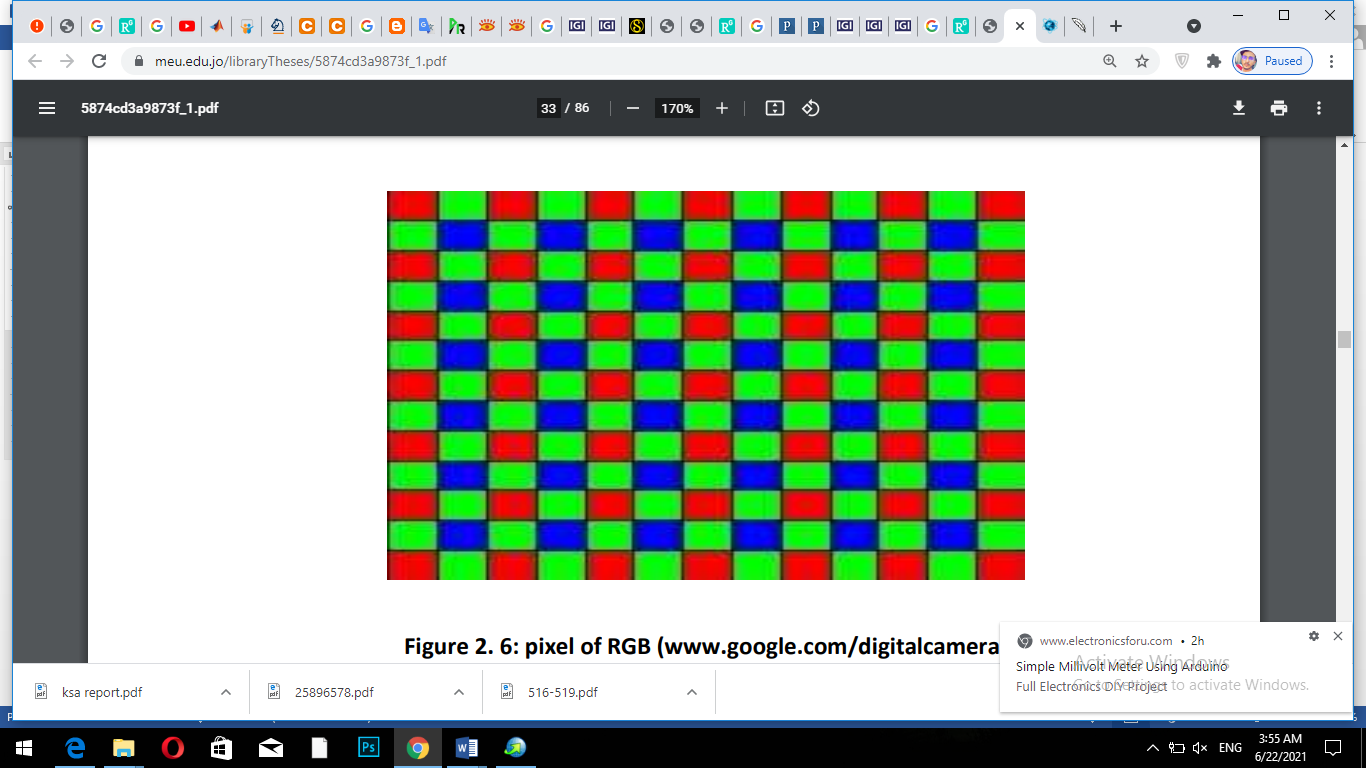
Nowadays, information security is a big problem in our community. Cryptography is a powerful information security tool. However, the main problem with cryptographic systems is to keep the keys secret. These images are very sensitive, and intruders may suddenly decipher them. In the current environment, maintaining the security and confidentiality of image data is a key issue (Delfs and Kneeble, 2007). Each image is composed of small elements called pixels. These pixels are aligned. Pixels have the same attributes as the original image, and each pixel represents a small part of the image. When scanning an image with a scanner or digital camera, the image is divided into towers and columns of small pixels, and each pixel is transmitted.

When encrypting, these pixels are assigned three colours these pixels are arranged in three colours of red, green, and blue. If they are encrypted, replace and transpose are added, the original position will be changed, and the numbers will be changed to a new order. The goal of compulsory encryption of images by implementing random multiple systems is to increase Keys pace. Therefore, this key makes it very difficult to crack the encryption. However, it turns out that both the number of calculations and the number of encryptions are large, so the pixel value and position are changed to increase the blurriness of the encrypted image.

It has been set up that the majority of chaos based image encryption algorithms primarily based totally bewilderment and drift methodologies. The cognitive dissonance technique shuffles the locations of pixels in a simple image, resulting in a visually disorganized and unidentifiable image. By changing the gray values of pixels, the diffusion method modifies the statistical properties of pictures. So, that is the resulting means of enhancing the grey values of pixels as figure 2.6 is illustrate different pixel of RGB color.

### Image Cryptography and Image Steganography

Figure ‎0.5: Pixel of RGB.



Cryptography allows data to be safely and discreetly sent from one end to the other. Cryptographic technologies are widely employed to maintain the identity and validity of sensitive information.. Steganography is the hiding of one message in another, which can only be recognized by the recipient. In any communication, security is an urgent issue in the modern world. Many privacy and steganography algorithms have been developed in the past. Ten years, and as the driving some idea to apply our requirement in the research.

Steganography is the act of concealing a message within another message in such a way that only the intended receiver able detect it. In today's society, security is a critical problem in any communication. Many data security and steganography techniques have been developed in the last decade, which inspired our analysis. The technology was created to allow the typical user to safely send confidential messages.

### Randomness

Random numbers can be used to generate encryption images, and model complex phenomena, and select random samples from large data sets. Random number generation includes two main methods: pseudo-random number generator (PRNG) and true random number generator (TRNG). They have input digitized some real analogy sources, such as microphone sound and audio. With enough magnification, it can detect anything (SivakumarandVenkatesan, 2016).

Once a user hits a button, it generates and displays numerous random pictures at the same time that will allow to make a button using the HTML code Generate Image. These photos will be saved in an array chosen by the user. When a user clicks the Generate Image button, five random images are generated and shown on the webpage.

Steps below, how this will be done:

* Declare an array the usage of JavaScript and offer the hyperlink or URL of photos in that array to shop the photos.
* Use for any loop to generate a couple of random photos straight away. We will use for loop of zero to five to show 5 photos in an unmarried button click on.
* Put the under steps on this for a loop.
* Calculate a random quantity among zero to the period of the array the usage of the floor (Math. random()\*random image. period) method. This generated quantity will assign to the photos to show randomly.

Now, print all 5 random photos decided on the usage of a number of calculated within side the preceding step.

### Size of key

A cryptosystem should be sensitive to the key, which means that the cipher text should have a close connection with the key, according to the basic concept of cryptology. There are two methods to meet this requirement: one is to completely mix the key with the plain text throughout the encryption process, and the other is to utilize a good, randomized key. The length of a good key distinguishes it.

# 

# RESEARCH METHODOLOGY

## I**ntroduction**

This chapter will discuss about proposed methodology focuses on the encryption of BMP colour images. The image pixels are grouped into 16x16 blocks. The encryption process is performed using a crucial, which is a series of bytes divided into different colour by selecting in random. Including the process of extracting the relevant string from the key, where the process of encrypting each cell in each image is performed by replacing and transposing X-O. This process is implemented in each cell of each block to achieve the ideal generation of a random key sequence number, so as to achieve the expected goal of a minimum key size of 2048 bits, and to fully encrypt the image. On the other hand, the progression of decrypting this image is carried out in reverse order. It might be suggested method is implemented by using various simulations such as writing the C# programming language in order to figure out the output results. The resulting output is estimated based on the signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR), normalized root mean square error (NAME) and processing time. By evaluating the encryption speed and the amount of encrypted data, these measures are selected based on their proven reliability.

**Input image**

**Generate the secret key as block**

**Divide image into blocks of size**

)

**Divide image into colour**

)

**Diffusion operation**

)

**Confusion operation**

)

**Get encryption image**

)

The original image

Diffusion operation

Confusion operation

Divide encrypted image with blocks of selecting size and color

Use the secret of size key (16 \*16)

Encryption process

Decryption process

Figure ‎0.1: Diagram of the proposed algorithm.

## Methodology and the Proposed Work

Yes

**Table 3.‎0‑1:** **: Characteristic of Power Quality Signal**Yes

Based on figure 3.1, the system design first determines image input so, the suggested approach encrypts images utilizing basic transposition and substitution operations, as well as algorithms, to provide a high-security encryption and decryption solution for random images. The proposed approach will employ a proportionately big secret key in the form of a byte matrix of size (16 × 16). (Represented in hexadecimal number system). This key is used for transposition and replacement operations, and provides good obfuscation and propagation characteristics in an encrypted form. Image. As some literature studies have shown, the security level of the bias module is very low. In image encryption, if the histogram of the mixed image does not change, it is sometimes invalid for statistical attacks. In order to improve the confusion weakness and the encryption process, this paper proposes a bit-level replacement method based on a specific confusion diffusion effect. Based on the inactive obfuscation and diffusion module, based on the transposition and replacement of the original image. This process will be performed multiple times according to the size of the private key: the original image is divided into (16 x 16) pixel-sized blocks. The overall overview of the method is shown in figure 3.1, the architecture of the encryption phase is shown in figure 3.2, and the architecture of the decryption phase is shown in figure 3.

**Source image**

**Divide the image into M blocks of size**

**Divide the secret key into M block of size 256 bytes**

**Start with the first block**

**Start with the first block**

**Diffusion operation XOR by bits of each block depend on the color image and the size of image**

**Encrypted image**

**Confusion operation depend on secret key blocks of any image and select the right image which match with requirements**

**Confusion operation depend on secret key blocks of any image and select the right image which match with requirements**

**Block concatenation**

\*NOTE: Where M blocks is the Source image size / Secret key (16×16) size

Repeat for M blocks

Figure ‎0.2: The architecture and the methodology of the proposed encryption phase.

To illustrate the proposed algorithm methodology, the following definitions and terminologies were proposed:

* **Secret Key (K):** series of bytes may represent any digital file such as image, sound, text, etc. The generation of the secret key is very important in order to achieve good protection for encrypted data. In addition, the length of the key is as large as possible, and there are as many random bytes as possible.
* **Key length (length):** the number of bytes in the key image.
* **Original image (S):** two-dimensional pixel bitmap palette encryption with width, height, and height the method processes the image file into a series of bytes, and the value of each byte ranges from (0 ... 255) to (1 byte = 8 bits). The bytes in the \*original image (S) are the same (width x height x palette).
* **Encrypted image (E):** The generated encrypted image forms the original S image, which is created after the encryption step is completed.

Table 3. 1: Sample of data block

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0  1 | B9  DC | D1  FE | C4  AD | 8E  50 | 34  D1 | 8F  D9 | E7  FD | 71  8 | FA  B3 | 46  86 | 4A  EF | 77  B0 | A1  8B | 78  14 | EB  2F | 7  74 |
| 2  3 | 4C  25 | FD  38 | A4  68 | C3  B7 | 7  9E | 61  7C | 57  31 | F5  E0 | 81  D3 | B7  BC | 1E  DB | 46  AE | E8  9F | CB  37 | 56  E5 | 75  E5 |
| 4  5  6 | 16  30  D2 | D6  7A  38 | 2B  8A  2F | A4  53  11 | D3  AB  9F | 38  77  B1 | FF  D5  A1 | 7B  CF  ED | A6  CB  38 | B8  C3  ED | CF  F0  11 | 19  4B  E6 | BA  85  AD | B7  A9  18 | 20  55  26 | E7  49  1B |
| 7  8 | 9C  63 | F3  85 | 7D  47 | 25  81 | AD  88 | 91  E | 39  47 | 9E  7E | 1  D8 | 5C  9C | D9  1A | F  BE | 48  66 | B4  EE | F5  21 | FD  B3 |
| 9  A  B | 9D  F8  3A | D4  13  26 | AF  83  72 | 91  27  73 | 2C  D0  5 | 2F  A4  63 | 9B  93  D0 | 40  8D  33 | FF  AC  E9 | 91  FE  7 | 10  4D  82 | 43  10  F6 | D7  77  EF | 91  7B  4 | 5F  37  A7 | 84  12  47 |
| C  D | F7  5A | 96  FD | C5  8 | 52  B1 | 6B  1F | F9  31 | E2  7F | F9  94 | 41  42 | 21  4F | E5  3D | 2D  C8 | E2  22 | 8B  9C | C8  8F | 83  A7 |
| E  F | 57  3E | 5  FE | 18  9C | E0  0 | B5  FB | E4  F6 | A6  28 | 41  C5 | 43  17 | 79  30 | 32  10 | E3  1C | 7D  BB | A3  1A | 51  D6 | 5F  A4 |

* **Decrypted Image (D):** Decrypted Image, derived from Image E, generated by encrypted Image E.
* **Logic XOR:** A logical operation that uses encryption and decryption stages to change the byte position of an image string.
* **Secret Key Block (KB):** This is a secret key with a two-dimensional arrangement of secret bytes. The key array is a set of 256-byte keys.

The byte values ​​in the array are expressed in hexadecimal. Table 1: An example of a (16x16) KB key block is shown. Table 1: An example (16x16)

* KB secret Key block. KB (i, j): Represents the byte in the i-th row and j-th column in KB.
* Image Data Block (DB (b)): is a two-dimensional array (16 x 16) of the original image DB bytes (b) represents the number of bytes in the original image S (in the encryption step) or the encrypted image E (in the decryption step)
* DB (b, i, j): represents the byte in block b in the i-th row and j-th column
* . Next Element: represents A two-dimensional array of index pairs (r, c), each pair represents the rth row and cth column of the next element in the array. The determination of the next item is based on the KB value of the corresponding item.

1. When scanning array elements (row by row) from elements (0, 0) to (15, 15), the following will occur:

* If KB (i, j) is not selected as the next element before, and KB(i, j) = XY, where X and Y are the left and right digits of the hexadecimal value of KB (i, j). This means that the pair specified in Next Element is (i, j) = (X, Y)
* . If KB(i,j) is selected as the next element above, it means the pair set in Next Element(i,j)=(i,j). (i., there is no element after element (i, j))

Element matrix are:

* [0,0]-(B,9)-(0,7)-(7,1)-(F,3)
* [0,2]-(C,4)-(6,B)-(E,6)-(A,6)-(9,3)-(9,1)-(D,4)-(1,F)-(7,4)-(A,D)-(7,B)-(0,F)-(0,7)-(7,1)-(F,3)-(0,0)-(B,9)
* [1,8]-(B,3)-(7,3)-(2,5)-(6,1)-(3,8)-(D,3)-(B,1)-(2,6)-(5,7)-(C,F)-(8,3)-(8,1)-(8,5)-(0,E)-(F,B)-(1,C)-(8,B)-(B,E)-(A,7)-(8,D)-(E,E)-(5,1)-(7,A)-(D,9)-(4,F)-(E,7)-(4,1)-(D,6)-(7,F)-(F,D)-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)
* [1,9]-(8,6)-(4,7)-(7,B)-(0,F)-(0,7)-(7,1)-(F,3)-(0,0)-(B,9)
* [8,9]-(9,C)-(D,7)-(9,4)-(2,C)-(E,8)-(4,3)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)-(D,6)-(7,F)-(F,D)-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)
* [8,A]-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)-(D,6)-(7,F)-(F,D)
* [A,D]-(7,B)-(0,F)-(0,7)-(7,1)-(F,3)-(0,0)-(B,9)
* [A,E]-(3,7)-(E,0)-(5,7)-(C,F)-(8,3)-(8,1)-(8,5)-(0,E)-(F,B)-(1,C)-(8,B)-(B,E)-(A,7)-(8,D)-(E,E)-(5,1)-(7,A)-(D,9)-(4,F)-(E,7)-(4,1)-(D,6)-(7,F)-(F,D)-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)

The proposed encryption **approach** has **the subsequent** steps: -

**Step1:** Read (from the user) **the name of the game** key K of **duration** K Length.

**Step2:** Read (from the user) the **unique** **photograph** S of **duration** S Length.

**Step3:** Represent the **unique** **photograph** S as m **quantity** of blocks DB of size (16×16). Where: M = S Length / (16×16) and the set of blocks are: DB (**zero**) … DB (m-1)

**Step4:** Set Kind ex = **zero** and

**Step5:** For **every** **information** block DB from b=**zero** to m-1

* + - * 1. Read sequentially 256 bytes from the secret key Kand fill KB,(i.e., K(Kindex) … K(Kindex+256)). When Kind ex = K Length (end of the secret key), then set Kindex = 0 (return to the Beginning of the secret key).
        2. For each element in data block from DB(b, 0, 0) to DB(b,F, F)

1. Build Next Element Block matrix.
2. Perform the diffusion substitution operation by XORing the corresponding bytes in the DB (b) Based on the sequence of elements in the Next Element matrix. For the above example in Table 1, the value of DB (b, 0, 0) is coring with the key values as follow:

Assume the value of DB (b, 0, 0) = 6E.

|  |  |
| --- | --- |
| DB(b, 0, 0)=DB(b, 0, 0) XOR KB(0,0)  DB(b, 0, 0)=DB(b, 0, 0) XOR KB(B,9)  DB(b, 0, 0)=DB(b, 0, 0) XOR KB(0,7)  DB(b, 0, 0) = DB(b, 0, 0) XOR KB(7,1)  DB(b, 0, 0) = DB(b, 0, 0) XOR KB(F,3) | 1101 0111=0110 1110 XOR1011 1001  1101 0000=1101 0111 XOR 00000111  1010 0001=1101 0000 XOR 01110001  0101 0010=1010 0001 XOR 11110011  0101 0010=0101 0010 XOR 11110011 |

1. Perform the confusion operation by exchanging the corresponding bytes in the DB (b) based on the sequence of elements in the Next Element matrix. For the above example in Table 1, the value of DB (b, 0, 0) is exchanging with the values as follow:

* DB (b, 0, 0) DB (b, B, 9)
* DB (b, B, 9) DB (b, 0, 7)
* DB (b, 0, 7) DB (b, 7, 1)
* DB (b, 7, 1) DB (b, F, 3)

**Step 6:** Create the encryption picture E from the encrypted data blocks.

### Algorithm for the Decryption Phase

This algorithm will generate the origin image S from the encrypted image E; the stages that follow will explain the actions in this design of the plan approach in detail. The methods in the suggested decryption technique are as follows:

* Step 1: Read (from the user) the length of the secret key K.
* Step 2: Read the encrypted image E of length from the user.
* Step 3: Represent the picture E as m blocks of size (1616). M = Length / (1616) - and the set of blocks is: DB (0)... DB(m-1)
* Step 4: Make Kindex equal to 0 and
* Step 5: For each data block DB from b, repeat step 4.
* Read sequentially 256 bytes from the secret key Kind fill KB, (K (Kindex) … K (Kindex+256)). When Kindex = Length (end of the secret key), then set Kindex = 0 (return to the beginning of the secret key).
* For each element in data block from DB(b, 0, 0) to DB(b, F, F)

1. Build Next Element Block matrix
2. Perform the diffusion operation by exchanging the corresponding bytes in the DB (b) based on the sequence of elements in the Next Element matrix.
3. Perform the confusion operation by XORing the corresponding bytes in the DB (b) based on the sequence of elements in the Next Element matrix.

* **Step6:** Construct the source image S from the set of the decrypted data blocks.

## Measurements used to evaluate the proposed algorithm

Using the proposed encryption system with Data Encryption Standard (DES) and Advanced Encryption Standard (AES), a series of comparative tests were carried out on different images. During these tests, measurements such as signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), normalized mean absolute error (NMAE), and encryption time (time) are used to determine the performance and achievable security level for the System to detect random colour

### Image Histogram

An image histogram is a graphical depiction of an image's pixel intensity distribution. As a result, an image histogram shows how such pixels in an image are allocated by displaying the number of pixels at each intensity level.

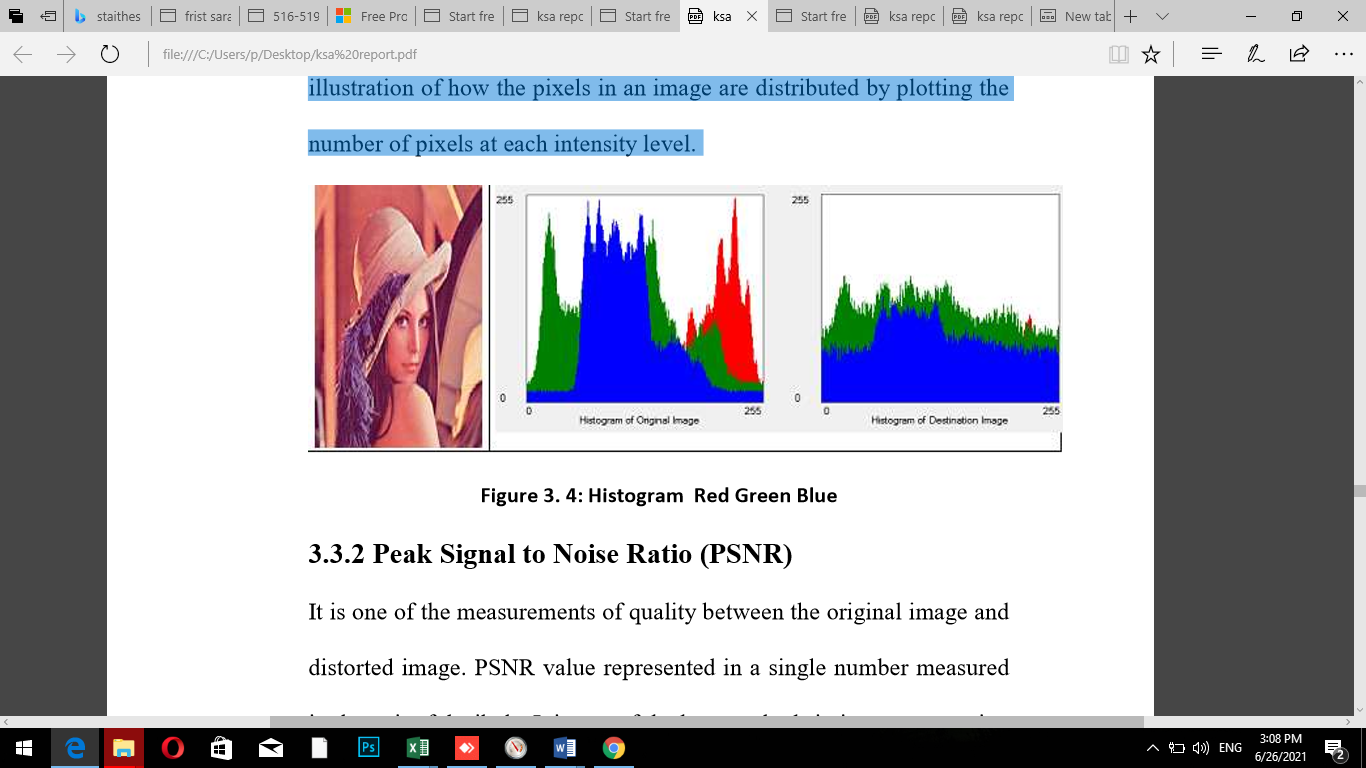


Figure ‎0.3: Histogram Red Green Blue.

### Peak Signal to Noise Ratio (PSNR)

It is a measure of the quality between the original image and the distorted image. The PSNR value is represented by a single number measured in decibels. It is one of the best machine vision analysis methods to measure the ratio of raw data. Distorted (noise) data in encrypted images. A low PSNR indicates the effectiveness of the encryption algorithm. As can be seen from the figures obtained, the difference between them is one-tenth. As mentioned earlier, these numbers represent the proportion and quantity of encrypted data. Therefore, any small change in the number will result in a huge change in the encryption result.

# 

# RESULT AND DISCUSSION

## Implementation

The encryption and decryption methods were written in C#, and they were tested. The tests are carried out utilising bit mapped (BMP) pictures of varying sizes and 256 colours, which are used in the experiments. Different types of pictures were used to assess the encryption and decryption procedures on the photographs. Images as well as a variety of hidden keys have been used. The outcome analysis is as follows:

The investigation was carried out for four distinct samples of pictures and four distinct secrets, the visual assessment of the histogram is critical in the evaluation of the findings. Standard assessment of the picture, as well as standard evaluation utilising standard measurements such as the Peak Signal to Noise Ratio (PSNR), the Signal to Noise Ratio (SNR), and so on (SNR), the Normalized Mean Absolute Error (NMAE) and the timing of the encrypted data are both important as well as the decrypted image.

When calculating the value of the PSNR, the following equations are employed:

In terms of the NMAE, the following equations are employed:

## System specification used

In this study, a computer system according to the following specifications was utilised to develop and test the proposed picture encryption method:

* PC with an Intel Core i7 processor
* HD (0.5 TB),
* RAM is 4.00 GB in size.
* HD Graphics VGA (High-Definition Graphics)
* Windows 7 Professional, 64-bit operating system.

## The Expected results

By doing the experiment with the aforementioned four pictures of varying sizes of type (.bmp), as indicated in Table 4.1 below, the results were obtained.

Table ‎0‑1: Images used in experiments

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Name | Lena | Baboon | Pepper | Balloon |
| Size | 128\*128 | 128\*128 | 128\*95 | 128\*128 |

Figures 4.1, 4.2, 4.3, and 4.4 show the histogram results of an encrypted sample picture that was created using the suggested method.

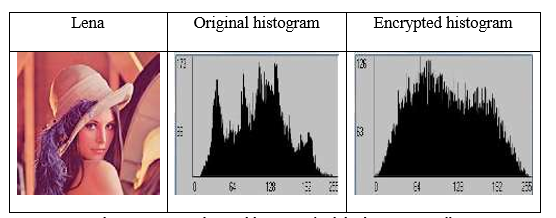


Figure ‎0.1: Lena image histogram (Original & Encrypted).

Despite the fact that the Lena picture contains a large amount of data, it has been heavily encrypted and the majority of the original image has been processed.

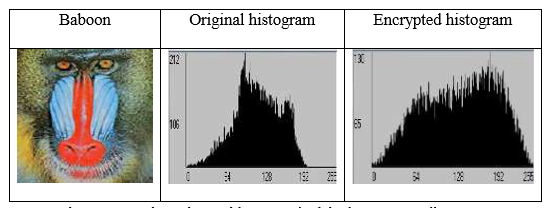


Figure ‎0.2: Baboon image histogram (Original & Encrypted).

Despite the fact that the baboon picture contains a large amount of data, it has been heavily encrypted and the majority of the original image has been processed.

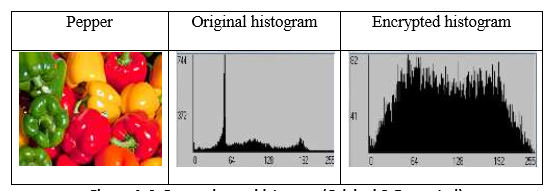


Figure ‎0.3: Pepper image histogram (Original & Encrypted).

It is apparent from the histogram above that the encryption was accomplished to a high degree by decreasing the majority of the data and boosting the cyphered signal. This demonstrates the effectiveness of encryption. Despite the fact that the initial data set is of limited size, it is still useful.

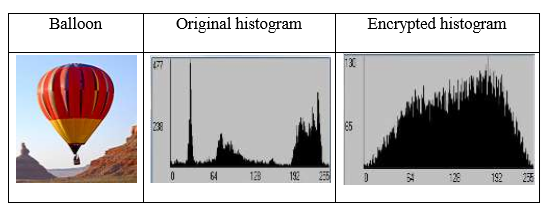


Figure ‎0.4: Balloon image histogram (Original & Encrypted).

The balloon picture histogram indicates a high data image, despite the fact that it was heavily encrypted and that the majority of the original image had been transformed.

### The Result of the Proposed Experiment

Table ‎0‑2: Proposed technique result.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Image | Secret key | SNR (dB) | PSNR (dB) | NMAE (%) | TIME(sec) |
| Lena | Text(27.4 )KB | 1.822 | 7.075 | 62.839 | 0.545 |
| Baboon | Audio(4.61)KB | 2.760 | 7.618 | 62.143 | 0.958 |
| Pepper | Image(4.19)KB | 0.016 | 4.899 | 103.253 | 0.402 |
| Balloon | Pdf (1.09)MB | 1.251 | 5.397 | 60.307 | 0.745 |

It can be seen in table 4.2 above that there is a direct relationship between the secret key file that was used and the results obtained. It should also be noted that the size of all pictures is maintained constant (up to 128), in order to avoid the influence of image size on the outcomes. It should be noted that the performance of image security is dependent on the size of the key and the number of blocks that have been used to create the secret key chain, which can be determined by the following formula:

The audio secret key on the baboon image with 4.61\*1024/256 = 18 (approximately) blocks produced which produces a (18\*2082 = 36864 bit (approximately) when using the text file with 27.4\*1024/256 = 109 blocks produced which produces SNR = 2.329 dB with 530 seconds compared to 2.760 with 0.958 seconds, indicating a significant difference in processing time. When using the text file with 27.

Referring to picture 4.3, which illustrates that data is sparse in comparison to figures 4.1 and 4.2, and the PSNR values given in the table, it can be seen that utilising the image key resulted in the lowest value of all, while using both the text and audio keys resulted in the greatest value.

The NMAE numbers indicate that the image secret key has surpassed 100 percent, whereas the other keys have values that are nearly as low as the image secret key (62. percent).

The time taken by each key demonstrated a significant difference, with the picture grin key taking the shortest amount of time (0.402 sec) and the audio key taking the longest amount of time (0.938 sec). As for the time, it should be noted that the pepper picture has the shortest time, while the baboon image has the longest duration.

To provide more clarification, two secret keys were used on the pepper picture to determine whether altering the key had any effect on the encryption process. The results of this experiment are shown in Table (4.3).

Table ‎0‑3: Using two different keys on the Baboon image.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| The Secret Key | Time (sec) | SNR (dB) | PSNR (dB) | NMAE (%) |
| Image (4190) byte | 0.527 | 2.785 | 7.721 | 61.274 |
| Audio (4720) byte | 0.958 | 2.760 | 7.618 | 62.143 |

Table ‎0‑4: Number of blocks in secret key.

|  |  |  |
| --- | --- | --- |
| The Secret Key | Size (byte) | Number of blocks |
| Image | 4190 | 16 |
| Audio | 4720 | 18 |

When comparing the picture and the audio, the number of blocks for the image is 16 blocks with a size of 4190 bytes, which results in 32768 key sizes when comparing the audio and the image (18 blocks, 4720 bytes, 35864). However, the numbers show that the image has better performance in terms of time because the number of blocks is less; however, the numbers also show that the SNR and PSNR and NAME showed stronger ciphering in baboon image duo to a larger number of blocks, which resulted in an increase in the number of chains, which resulted in a longer secret key, which achieved high performance in security.

Table ‎0‑5: Using two different keys on the Lena image.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| The Secret Key | Time (sec) | SNR (dB) | PSNR (dB) | NMAE (%) |
| Pdf(1.9) Mb | 0.601 | 2.172 | 7.269 | 61.254 |
| Text (27) Kb | 0.958 | 2.760 | 7.618 | 62.143 |

The number of blocks for the pdf is shown in the table above (1.9\*1024\*1024/256 = 4464). This results in a key size of 4464\*2084 bits, which is much longer than the text. This demonstrates that a large size was generated as a consequence of the measurements SNR 2.172 less than 2.760 with PSNR 7.269 less than 7.618 in 449 dB and SNR 2.172 less than 2.760. This resulted in increased chaos in the picture, resulting in great performance in terms of unpredictability of key and complexity, which in turn offers high security.

Table ‎0‑6: Using two different keys on the Balloon image.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| The Secret Key | Time (sec) | SNR (dB) | PSNR (dB) | NMAE (%) |
| Pdf(1.9) Mb | 0.745 | 1.251 | 5.397 | 60.309 |
| Text (27) Kb | 0.577 | 1.97 | 5.866 | 58.86 |

### AES Result

Table ‎0‑7: AES result.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image | SNR (dB) | PSNR (dB) | NMAE (%) | TIME(sec) |
| Lena | 3.922 | 8.03 | 62.436 | 0.166 |
| Baboon | 4.23 | 7.465 | 64.465 | 0.100 |
| Pepper | 1.832 | 6.494 | 65.695 | 0.96 |
| Balloon | 2.084 | 6.853 | 65.695 | 0.075 |

In part because of the strong algorithm in use, the AES method is a very effective ciphering technique. If the results produced from other methods are comparable to these results, the techniques' credibility will be enhanced. In accordance with Table 4.7, the following observations are made:

The SNR is a measure of the strength of a signal. The pepper picture is the least prominent, while the baboon image is the most prominent.

When it comes to PSNR, the Lena picture has the greatest value while the balloon has the lowest.

As for the MANE, the picture of pepper is the most prominent. While the lowest Lena picture is shown.

### DES result

Table ‎0‑8: DES Result.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image | SNR (dB) | PSNR (dB) | NMAE (%) | TIME(sec) |
| Lena | 3.887 | 7.981 | 62.753 | 0.207 |
| Baboon | 4.238 | 7.461 | 65.006 | .097 |
| Pepper | 1.841 | 6.488 | 104.003 | 0.70 |
| Balloon | 2.04 | 6.815 | 66.352 | 0.076 |

According to the data in the preceding table, the SNR value is greater in the balloon and lower in the pepper, while the PSNR value is higher in the Lena and lower in the balloon, and the NMAE value is higher in the pepper and lower in the balloon, respectively.

## Comparison among Technique

### SNR dB

Table ‎0‑9: PSNR in Proposed, AES and DES.

|  |  |  |  |
| --- | --- | --- | --- |
| Image | Proposed | AES | DES |
| Lena | 1.822 | 3.922 | 3.87 |
| Baboon | 2.76 | 4.23 | 4.238 |
| Balloon | 1.251 | 2.084 | 2.04 |

Because of this, it is much more difficult to distinguish between the proposed and other techniques in the table above. Also, considering that data contained in a balloon image affects the outcome and that the proposed algorithm differs from AES and DES, it is much more difficult to distinguish between these two techniques. In this case, the difference (.833) indicates that the picture has more chaos than the other systems.

### PSNR dB

Table ‎0‑10: PSNR in Proposed, AES and DES.

|  |  |  |  |
| --- | --- | --- | --- |
| Image | Proposed | AES | DES |
| Lena | 7.075 | 8.03 | 7.981 |
| Baboon | 7.618 | 7.465 | 7.461 |
| Balloon | 5.397 | 6.853 | 6.815 |

It is clear that the PSNR value is closely linked to the SNR values described in Table 4.10, and that the values of PSNR in the table are lower for the suggested method than for the other two techniques, which is consistent with previous findings.

### NMAE

Table ‎0‑11: NMAE in Proposed, AES and DES.

|  |  |  |  |
| --- | --- | --- | --- |
| Image | Proposed | AES | DES |
| Lena | 62.839% | 62.436% | 62.753% |
| Baboon | 62.143% | 64.458% | 65.006% |
| Balloon | 62.307% | 65.465% | 66.352% |

When looking at the NMAE variant values in Table 4.11, it is clear that the ratios in the three methods are almost identical. This demonstrates that the suggested system has the same amount of power as the AES and DES algorithm methods. Furthermore, in order to demonstrate the effectiveness of the proposed method in comparison to DES, AES images of varying sizes will be subjected to encryption using the three algorithm strategies suggested. Tables 4.10 and 4.11 illustrate the outcomes of the experiment.

Table ‎0‑12: Sizes of images and secret keys.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image | Lena | Baboon | Pepper | Balloon |
| Size image | 250\*265 | 200\*128 | 640\*480 | 200\*200 |
| Secret key | Text file 27.kb | Audio 48.kb | Image 4.19 kb | Pdf 1.09 Mb |

Table ‎0‑13: Comparison results between Proposed and AES with different sizes images

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PROPOSED | | | | | AES | | | |
| Source Image | SNR dB | PSNR dB | NMAE % | TIME sec | SNR dB | PSNR dB | NMAE % | TIME Sec |
| Lena | 1.882 | 7.05 | 62.66 | 1.92 | 3.878 | 7.669 | 63.139 | 0.35 |
| baboon | 1.11 | 5.419 | 62.06 | 0.498 | 2.672 | 6.842 | 65.999 | 0.70 |
| pepper | 0.937 | 5.026 | 62.623 | 0.498 | 1.895 | 6.561 | 61.662 | 0.88 |
| balloon | 2.556 | 7.438 | 60.532 | 5.382 | 3.93 | 8.481 | 63.378 | 0.35 |

When examining the data in the preceding table, it is discovered that the values obtained when applying the proposed technique are better than those obtained when applying the AES algorithm technique, thereby supporting the notion previously stated that the proposed algorithm technique is powerful and reliable.

## Security Analysis and discussion

A large number of tests were carried out in order to assess the suggested encryption technique, utilising three bitmap pictures of type (.bmp) that were of varying sizes. On the proposed image encryption method, some security analyses have been carried out. These include the most important ones such as key space analysis, key sensitivity analysis, and statistical analysis, all of which have been carried out to demonstrate that the proposed method has good security features.

### Experimental Results and Security Analysis

The suggested algorithm approach was subjected to a security study, which included key space analysis, key sensitivity analysis, and statistical analysis, in order to demonstrate that the proposed method has excellent security features.

#### Key Space Analysis

The key space is the single most important element in determining the resilience of ciphering algorithms. The following formula may be used to locate the key space:

The dimension of the block is 16\*16 inches in this case. 8 is the colour palette of red, green, and blue, and K is the number of blocks that can be determined by dividing the secret file's size by 256.

The sequence of procedures produced huge space key chains that provided a sufficient level of complexity and unpredictability to guarantee that the picture was of good quality chaos, as seen in the figure 4.5.

#### Key Sensitivity

In order to investigate the key sensitivity characteristic of the suggested algorithm method, a one-bit modification is made to the secret key, which is then utilised to decode the encrypted picture after it has been encrypted. When comparing the encrypted picture obtained with the incorrect key to the decrypted image obtained with the right key, as shown in Figure, it is clear that the incorrect key was used (4.5). This establishes that the suggested encryption technique is very sensitive to the key in such a manner that even an almost perfect guess of the key does not compromise its effectiveness.

Disclose any information about the simple picture that has been hidden

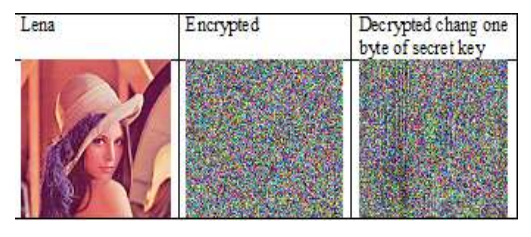
****

Figure ‎0.5: Decrypted Lena image using wrong key.

## Robustness and level of security

### Robustness

The suggested algorithm method has proved to be effective owing to the lengthy key that has been integrated into the system, which results in the formation of chains of elements that change in position and value, resulting in overlapping of the components.

### Security image

A technique of picture encryption produced information that was unreadable; as a result, no unauthorised person had access to the original image or any other kind of sending information over public networks. The technology provides a strong level of privacy and safety.

# 

# CONCLUSION

## Introduction

In this object, a new algorithm is proposed, which adds important value to the proposed image encryption technology. This algorithm proposes an image encryption technology that uses a key chain with a minimum size of 2048 bits (16 \* 16 \* 8); therefore, the original image consists of a series of pixels, which are divided into continuous byte blocks. A series of unconventional replacement and transposition processes are performed pixel by pixel, creating a long, complicated, and random key. This provides a high level of protection for encrypted images. The encryption algorithm uses bitmaps effectively.

In this labour, the proposed model was tested on four images (Lina, Baboon, Pepper, and Balloon). The purpose is to test the strength of the private key. The following four measures are used:

1. The signal from the original data to the corrupted encrypted data. (The lower the SNR value, the better the encryption effect), the result shows:

* Proposed: 0.016 dB to 2.76 dB
* AES: from 1.844 decibels to 3,922 decibels.
* DES: 1,844 dB to 4,258 dB

1. (SNR values with inside the proposed approach display higher cost than AES, DES). The Peak Signal to Noise Ratio (PSNR) - is a ratio that suggests the PSNR, as SNR (the much less than the cost of PSNR, the higher encryption got). The values showed:

* Proposed: From 4.899 to 7.075
* AES: From 6.494 TO 8.03
* DES: From 6.488 to 7.981

1. Normalized absolute mean error (NAME): This is a measure of encrypted data. The higher the NAME value, the better the encryption. The results obtained show:

* Proposed = 103.253% to 62.839%.
* AES = 62.436% to 65.956%
* DES = 62.753% to 66.352%.

In addition, it is observed that the proposed algorithm achieves good results in all experiments, with higher certainty and less time. This work uses images (Lena, Pepper, and Baboon) to show the difference between the original image and the encrypted image. Image. Finally, by comparing the work related to this research, it is found that the method used in this research is more reliable due to the longer key, its complexity and randomness.

The results show that the performance of the proposed algorithm is good, time is a measure of encryption time, and there is no significant change in the values ​​between the methods. The results show that the proposed algorithm has high PSNR, ANN and timeliness execution, transforming into a reliable and highly secure system

References

Ahmad, S. Alam, K. M. R. Rahman, H., and Tamura, S. (2015). A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. In Networking Systems and Security (NSysS), 2015 International Conference on, 1-5

Al-Husainy M. (2012). A Novel Encryption Method for Image Security, International Journal of Security and Its Applications, 6(1), 1-8

Auyporn, W. and Vongpradhip, S. (2015). A Robust Image Encryption Method Based on Bit Plane Decomposition and Multiple Chaotic Maps.

BaniYounes M. A. and Jantan, A. (2008). Image Encryption Using Block-Based Transformation Algorithm IAENG. International Journal of Computer Science, 35.

Boneh, D. Di Crescenzo, G. Ostrovsky, R. and Persiano, G. (2004).

Public key encryption with keyword search. In Advances in Cryptology-Eurocrypt. Springer Berlin Heidelberg, 506-522.

Chang, C. Hwang, M. and Chen, T. (2001). A new encryption algorithm for image cryptosystems, The Journal of Systems and Software 58, 83-91.

Delfs, H. and Knebl, H. (2007). Symmetric-key encryption Introduction to cryptography: principles and applications. Springer.

Guo, J., Ling, S., Rechberger, C., and Wang, H. (2010). Advanced meet in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. In Advances in Cryptology-ASIACRYPT 2010, Springer Berlin Heidelberg, 56-75

Kaur, N. and Singh, H. (2012). Efficient and Secure Data Storage in Cloud Computing Through Blowfish, RSA and Hash Function.

International Journal of Science and Research (IJSR), 4 (5) Lindner, R. and Peikert, C. (2011). Better key sizes (and attacks) for LWE-based encryption. In Topics in Cryptology–CT-RSA 2011,

Springer Berlin Heidelberg, 319-339 Microsoft Corporation all rights reserved. (2005), Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements, (WSE) 3.0 Reader, M. and Salam, K. (2014).

Image Encryption and Decryption Using Selective Block Encryption Technique, International Journal of Computer Science & Engineering Technology (IJCSET), 5(09), 1-8.

Sathish, K. BhoopathyBagan, K. and Vivekanand, V. (2011). A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems. Procedia Computer Science, 3, 378–387.

Sivakumar, T. and Venkatesan, R. (2013). A Novel Image Encryption Approach using Matrix Reordering. WSEAS Transactions on Computers, 12(11), 407-418.

Song, C. and Qiao, Y. (2015). A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. Entropy, 17 Wadi, S. M. and Zainal, N. (2013). Rapid Encryption Method Based on AES Algorithm for Grey ScaleHD Image Encryption. Procedia Technology. 4th International Conference on Electrical Engineering and Informatics, ICEEI, 11, 51–56.

Yang, G. Yu. Pan, Q. Sun, S. and PengXu. (2015). Novel Image Encryption based on Quantum Walks. Scientific Reports, 5 (7784).

Yun-peng, Z. Wei, L. Shui-ping, C. Zheng-jun, Z. Xuan, N. and Wei-di, D. (2009). Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics.

Chen, G. Mao, Y. and Chui, C. K. (2004). Design of Image Security System Based on Chaotic Maps Group system (A Novel Approach for Image Encryption using Dynamic SCAN Pattern, International Journal of Computer Science 41, 2