A Novel Design of Blowfish Algorithm for Image Security

Ashwaq T. Hashim 1, Ammar H. Jassem 2, Suhad A. Ali 3

1Department of Control and Systems Eng., Universitas of Technology-Iraq, Baghdad, Iraq
2,3Department of Computer Science, Science College for Women, University of Babylon, Iraq

Emails: suhad.ali2003@yahoo.com

Abstract. In order to improve the security and efficiency of image encryption systems comprehensively an image encryption based on enhanced design of Blowfish scheme is proposed. The proposed system is employed block based image encryption technique combined with chaotic map properties. Firstly the digital image is scrambled and decomposed into several key based blocks randomly to decorrelated the relationship between original and processed image then each block is passed through an enhanced blowfish algorithm. The enhancement in design is to gain advantage of the strong facility, which is maintained by blowfish algorithm by overcoming its flaws, which leads to a significant improvement in security/performance. As a result the proposed system offers good performance for image encryption. The proposed algorithm is 320-bit Blowfish-like block cipher, where cascaded looking composition of F-functions is used instead of rounds. The key is accepted a variable length up to 400 bytes. The pragmatic aim of the proposed system is to decrease memory requirements and execution time while keeping the cipher simple and highly adaptable to future demands. To ensure improved encryption algorithm, the implementation of both techniques has been carried out for experimental purposes which is showed that the original image has a flat histogram after encrypted, a decreasing correlation between adjacent pixels in all color components and increasing entropy for the cases studied. The proposed algorithm has a sufficiently large key space and a very high sensitivity to the key. A comparative study with previous Blowfish algorithm shows the superiority of the modified algorithm.

1. Introduction

In nearly all our lives areas the visual information and images play a significant profession. Due to the significant growth in the computers usage, there is growing tendency for security of image and fidelity authentication. Transferred images are possessed various applications, like commercial, military, and medical applications. Therefore it is essential to cipher the data of image before it is sent through the network for preserving its security and avoid unlicensed access. Nevertheless, compared with text, further processing power and
bandwidth are necessitated [1]. Image security is an application layer technology to protect the send information against unwanted exposure besides to safeguard the data from alteration while in transfer. It comprises numerous aspects such as copyright protection, authentication, confidentiality and access control. Conventional cipher algorithms are said to be undesirable for ciphering images for two reasons. One is that the image size is always more than text size. Therefore, traditional cryptography takes longer time to encrypt the image data. The other is the high correlated and redundancy of adjacent pixels of an image [2].

Although simple encryption is sufficient to protect digital images and videos in some civil applications, this issue has been taken into account when designing advanced encryption algorithms especially for sensitive digital images and videos. Images have special features are completely different from texts. Current research activities in the field of nonlinear dynamics and particularly on systems with complex (chaotic) behaviors [3] have forced many investigations into possible applications of these systems. Today, chaotic encryption is almost exclusively considered inside the nonlinear systems community [4].

In order to protect digital images from unauthorized users doing illegal reproduction and modifications, a variety of image encryption schemes are proposed.

In 2010, Alireza and Abdolrasou [1] proposed an image encryption system based on grouping of shuffling of pixel and an amended simplified AES version. Chaotic baker’s map is employed for shuffling and enhancing S-AES effectively by S-box design. Chaos is employed to increase diffusion and confusion in the image. Bora et al., in 2015, proposed a double encryption technique using Blowfish algorithm and Cross chaos map [5]. Jawad and Sulong, in 2015 [6], improved the level of security for the traditional Blowfish algorithm (BA) to cipher color image by changing it with new F-function. The dynamic S-box and XOR operator are produced from the F-function via 4D hyper-chaotic map, and the number of iterations is greatly reduced from 16 to 4 for simplify the processing complexity. The block secret keys of varying space size are randomly produced. Gowda [7] in 2016, an innovative method is introduced for more security, the first step is encrypting the data using Blowfish algorithm, then type encrypted data is divided into smaller number of blocks and random number of blocks are chosen to hide the encrypted blocks, to get the correct sequence of blocks hash tables are main tained. In 2017, Ross and Josephraj [8] modified the Blowfish algorithm by enhancing its performance in terms of speed, Throughput, Power consumption and Avalanche effect. they proposed a way to enhance the performance of the Blowfish cryptography algorithm by introducing parallel processing technique and making modifications to the Fiestel (F) function of Blowfish by combining the Blowfish and the Runge-kutta (RK) Method. The F function of Blowfish has been modified with different formulae and the outcome of a series of RK-Blowfish algorithms were compared with the Blowfish algorithm. Patel and Panchal [9] in 2017, an image cipher method is proposed rely on the two distinct encryption procedures, used to safeguard various images types. Compared with the single chaotic map scheme, the suggested algorithm may show higher security. Since using the similar structure to the Feistel block cipher the algorithm can complete the ciphered of two pixel blocks simultaneously which helps to increase data throughput. In 2017, Kanagalakshum and Mekala [10], designed a method based on Blowfish algorithm with improved features. It is used a supplementary key approach to strengthen the security of image. In 2018, Zhu et al. [11], an image encryption system is presented, which contains three main stages: padding pixels around the image, scrambling of pixel and diffusion pixel. At first, the hash value of the plaintext image is converted into a pseudo-random sequence, then adding pseudo-random sequences to the surrounding area of plaintext images. Then, adding pseudo-random sequences to the surrounding area of plaintext images. The pseudo-random sequences used in the permutation and diffusion process are related to the plaintext image. Huang et al., [12] in 2018 a simple chaotic color image encryption is presented. it used both plaintext related permutation and diffusion. In the permutation stage, the values of the parameters of cat map are related to plain images. It means that different original images correspond to different parameters. Thus, the permutation stage is related to plain image.
Zhang and Wang [13] in 2018 presented an image encryption algorithm with AES and chaos. Ashwaq and Yossra [14] in 2018, presented an enhanced algorithm for image encryption is presented by using improving four encryption algorithms Blowfish, TEA, RC6 and AES to encrypt color images. One feature of presented a BK-Cube Network algorithm is using a cube network design where the cube looking composition of F-functions is used instead of rounds. Li [15] in 2019 suggested an image encryption scheme, which is based on the three-dimensional chaotic logistic map. Ramasamy [16] in 2019 proposed a key generation algorithm that uses block scrambling, modified zigzag transformation, and enhanced logistic–tent map for image encryption.

The organization of this paper is as follows: Section 2 presents the related works represented by Blowfish and the chaotic logistic map; Section 3, the structure of proposed algorithm (include encryption and decryption) is explained. The experimental results are introduced in Section 4. Finally, the conclusions are shown in Section 5.

2. Proposed System

To date, many data-encryption methods are suggested and commonly utilized, like AES, Blowfish, RC5, RSA, or IDEA. Most of them are employed for binary text file or binary data. These methods are difficult to use directly in multimedia data and is ineffective to encrypt color images due to the high correlation between pixels. Multimedia data is often high-frequency and requires real-time interactions. To dispel the high relation among pixels and raise the entropy value, an algorithm based on enhanced Blowfish combined with chaotic map is proposed where the chaotic is used as preprocessing step. Firstly the digital image is decomposed into several key based blocks randomly to decorrelated the relationship between original and processed image then these blocks are passed through an enhanced blowfish algorithm. The enhancement is design to take advantage of the powerful facility, which is supported by blowfish algorithm with overcoming its weaknesses, resulting in a much improved security/performance trade off. As a result the proposed system offers good performance for image encryption. The proposed algorithm is 320-bit Blowfish-like block cipher, where cascaded looking composition of F-functions is used instead of rounds. The key length is variable to 400 bytes. Beside the increased security, the pragmatic aim of the proposed system is to decrease memory requirements and execution time while keeping the cipher simple and highly adaptable for future demands. Figure 1 illustrates the block diagram of proposed algorithm.

![Figure 1 Block Diagram of the Proposed System](image)
The algorithm (1) is presented the general steps of the proposed system.

| **Algorithm 1: Proposed Image Encryption** |
|-------------------------------------------|
| **Input:**                               |
| $I$, // RGB color image $I$               |
| $W, H$, // width and height of $I$        |
| **Secret Keys** //initial values and parameters for chaotic system |
| **Output:**                              |
| Encrypted Image $IE$.                    |

**Step 1:** Separate the color image $I$ into three subbands $IR$, $IG$, $IB$.

**Step 2:** The band matrices $Ir$, $Ig$, and $Ib$ are converted to a one dimensional vector

- $Ir = \{ IR (1), IR (2), \ldots, IR (l) \}$,
- $Ig = \{ IG (1), IG (2), \ldots, IG (l) \}$,
- $Ib = \{ IB (1), IB (2), \ldots, IB (l) \}$,

where $l = W \times H$

**Step 3:** Generate the three chaotic sequences $S_i$ where $i=1,...,6$ of length $l$ based on quadrature map using Secret Keys.

**Step 4:** Apply the proposed scrambling algorithm using generated chaotic sequences $S_i$ where $i=1,...,6$ on $Ir$, $Ig$, and $Ib$ to scramble the image pixels. This process is performed by two levels of scrambling and save the result in $BlockR$, $BlockG$, and $BlockB$ using algorithm (2).

**Step 5:** Apply the Enhanced Blowfish encryption algorithm using secret key $K$ on $BlockR$, $BlockG$, and $BlockB$ to get encrypted sub image $IE_r$, $IE_g$ and $IE_b$ using algorithm (3).

**Step 6:** Combine $IE_r$, $IE_g$, and $IE_b$ to generate output encrypted image $IE$.

### 2.1 Image Scrambling Based on Chaotic Map

The security issue can be solved by the high correlation between pixels and the large capacity of the data when encrypting an image. In the proposed system, the image is scrambling based on the chaotic map by generating a random sequence using Quadratic chaotic mapping [4] which is employed to scramble image pixels then generate another sequence using another initial condition and parameter of Quadratic chaotic mapping and normalize the range of the chaotic sequence to $[1, 10]$ and thus dividing the image into 10 blocks accordingly as shows in Figure 2.

Figure 3 illustrates an example of the proposed scrambling method for $8\times8$ image based on Quadratic chaotic mapping.
Figure 2: The Proposed Scrambling Image  

Algorithm 2: Proposed Image Scrambling

| Step | Description |
|------|-------------|
| Step 1 | Let $L = W \times H$ |
| Step 2 | Generate random sequence using Quadratic map  
  Let $a = 0.5$, $X_0 = 0.15$,  
  $X_0 = a \times X_0^2$  
  For $i = 1$ to $L$  
  $X_i = a \times X_{i-1}^2$  
  End for  |
| Step 3 | Normalize the chaotic map $X$ array  
  $Max = L$, $Min = 1$  
  For $i = 1$ to $L$  
  $S_{i1} = (Max - Min)/(Max - Min) \times (X_i - Max) + Max$  
  End for  |
| Step 4 | Replace recurring number with missing number of $S_i$ |
| Step 5 | An image pixel values are scrambled according to $S_i$ array locations |
| Step 6 | Convert the 1D array to 2D image matrix to get $IC_r$  |
| Step 7 | Generate another random sequence $S_2$ using Quadratic map with another initial condition $X_0$ and $a$  |
| Step 8 | Normalize the chaotic map $X_2$ array  
  $Max = 10$, $Min = 1$  
  For $i = 1$ to $L$  |
\[ S_i = \frac{\text{Max} - \text{Min}}{(\text{Max} - \text{Min})} \times (X_i' - \text{Max}) + \text{Max} \]

Step 9: Divide the scrambled image \( IC_t \) into 10 sub blocks \( \text{block}_R_i \) where \( i=1,..,10 \) according to \( S_2 \) array

Step 10: Repeat steps from 1 to 9 for \( I_g \) using secret parameters \( X1_0, a_1, X1'_0, a'_1 \) and consequently generated two random sequences \( S_3 \) and \( S_4 \) to output \( \text{block}_G_i \)

Step 11: Repeat steps from 1 to 9 for \( I_b \) using secret parameters \( X2_0, a_2, X2'_0, a'_2 \) and consequently generated two random sequences \( S_5 \) and \( S_6 \) to output \( \text{block}_B_i \)

2.2 Modified Blowfish Algorithm

The block size of traditional Blowfish algorithm is 64 bits [17] and this makes it vulnerable to birthday attacks, especially in contexts like HTTPS. In 2016, the SWEET32 attack showed how to take advantage of birthday attacks to perform invisible text recovery (i.e. decrypted text) against 64-bit block size [18]. The GnuPG project recommends that Blowfish not be used to encrypt files larger than 4 GB Because of the small size of the block [19]. The modified Blowfish algorithm has been enhanced by several techniques; firstly the block size and key length are increased to resist the birthday, matching and brute force attacks, secondly the key dependent permutation has been used to provide the necessary diffusion and confusion of the input block so that added differences are destroyed when the key alter. The modified Blowfish algorithm used one round of RC6 to input block as a reversible mixing function which is a more complicated. The previous blowfish algorithm used XOR as a reversible mixing function before the first and after the last round. The RC6 has been further confusing the entry values into the Substitution-Permutation Network (SPN) of proposed \( F \)-function and ensure a complete avalanche effect. The modified Blowfish algorithm is depicted in Figure 4

![Figure 4. The Modified Blowfish Algorithm](image)

Modified Blowfish is Blowfish-like block cipher. The plaintext is 320 bit which is divided into 10 parts \( \text{Block}_i \) where \( i=1..10 \). Each of part is 32 bits. The \( F \) function in proposed scheme will be used the cascaded design instead of rounds. The output is 320 bits \( E_i \) where \( i=1..10 \) of 32 bits. Algorithm of enhanced Blowfish algorithm is showed in algorithm (3).

The decryption operation of proposed algorithm is the inverse of the encryption operation and the code for decryption is similar.
2.2.1 The Design of F-function

The structure of proposed F-function is a usual Substitution-Permutation Network (SPN), which is also employed in numerous block ciphers, e.g. AES, Twofish, Serpent and RC6. In our first estimation for obtaining a reasonable margin of security and asymmetric iteration, the cascaded design choose the size of block and dependently determine the minimum number of rounds $N_r$ of the first output $E_1$ as 12 while the maximum $N_r$ as 30 for last output $E_{10}$. It is may be safe to decrease the iteration numbers from 16 to 8 without compromising security [20]. The iteration numbers essential for security may depend on key length. As seen with the current subkeys construction procedure, a 12-iteration algorithm cannot accept a key longer than 3200 bits compared with traditional blowfish which is accept key longer than 768 bits. Figure 11 shows the architecture of F-function which is took four inputs and four outputs and ten additional integer parameters represented subkeys. A more difficult integrating function is used to avoid symmetries. One round of RC6 [21] is employed as a reversible mixing function which is a more complicated reversible mixing function compared with XOR which is used as reversible mixing function before after the FB functions. Algorithm (4) lists the steps of the F function.

| Algorithm 3: Enhanced Blowfish algorithm for image encryption |
|---------------------------------------------------------------|
| **Input:** BlockR, BlockG, BlockB // Permuted blocks (i.e., each one is 10 //subblocks) |
| BlockR, BlockG, BlockB // Width and Height of input image |
| **Output:** E // Encrypted image |
| **Step1:** For i=1 to WxH step 10 |
| F (BlockR1, BlockR2, BlockR3, BlockR4, e1, e2, e3, e4) |
| F (BlockR5, BlockR6, e3, e4,) |
| F (BlockR7, BlockR8, e7, e8) |
| F (BlockR9, BlockR10, e11, e12, E1, E2) |
| . |
| . |
| . |
| End |
| Store BlockRi, i=1, ..10 in encrypted image E. |
| **Step2:** Repeat step1 for BlockG |
| **Step3:** Repeat step1 for BlockB |

Figure 5. The F function of the Proposed System
Algorithm 4: F function

| Input: | Block1, Block2, Block3, Block4 |
| --- | --- |
| Output: | e1, e2, e3, e4 |

**Step 1:**
- Block2 = Block2 + K0
- Block4 = Block4 + K1
- \( t = (\text{Block2} \times (2 \text{Block2} + 1))<<<\text{lgw} \)
- \( u = (\text{Block4} \times (2 \text{Block4} + 1))<<<\text{lgw} \)
- Block1 = ((Block1 XOR t)<<<u) + K2
- Block3 = ((Block3 XOR u)<<<t) + K3
- \((\text{Block1}; \text{Block2}; \text{Block3}; \text{Block4}) = (\text{Block2}; \text{Block3}; \text{Block4}; \text{Block1})\)

**Step 2:**
- T1 = FB(Block1)
- T2 = FB(Block4)
- Block2 = Block2 XOR T1
- Block3 = Block3 XOR T2
- \((\text{Block1}; \text{Block2}; \text{Block3}; \text{Block4}) = (\text{Block2}; \text{Block3}; \text{Block4}; \text{Block1})\)
- Block1 = Block1 + K4
- Block4 = Block4 + K5

**Step 3:**
- T1 = FB(Block1)
- T2 = FB(Block4)
- Block2 = Block2 XOR T1
- Block3 = Block3 XOR T2
- \((\text{Block1}; \text{Block2}; \text{Block3}; \text{Block4}) = (\text{Block2}; \text{Block3}; \text{Block4}; \text{Block1})\)

**Step 4:**
- Block2 = Block2 + K6
- Block4 = Block4 + K7
- \( t = (\text{Block2} \times (2 \text{Block2} + 1))<<<\text{lgw} \)
- \( u = (\text{Block4} \times (2 \text{Block4} + 1))<<<\text{lgw} \)
- Block1 = ((Block1 XOR t)<<<u) + K8
- Block3 = ((Block3 XOR u)<<<t) + K9

In the modified scheme Blocki is divided into four 8-bit quarters a, b, c, and d. Each quarter is indexed to the one of the S-boxes and entries to a single S-box are overlapped: entry 0 involves of bytes 0 through 3, entry 1 through 1 to 4, etc. This simplification will be decrease the requirements of memory for the S-boxes in traditional Blowfish algorithm from \(4 \times 4 \times 255\) (i.e., 4069 bytes) to \(4 \times 255\) (i.e., 1024). A more complex combining function in the proposed system is used to eliminate the symmetries represented by one round of RC6. Figure (12) depicts the FB function of proposed scheme.

In the design of the F function a combination of different operations is used in a way that will increase the advantages from each. Some of the characteristics of this function are:

a) The complexity of proposal algorithm will be increased by using combinations of basic operations. Hence by using F function a diffusion and confusion to the outputs of S-boxes are achieved. The permutations in proposed algorithm are key dependent so that it could avoid linking plaintexts to input to the first F function and ciphertexts to input to the last F-function. An F function will be used a combinations of basic operations to achieve a large number of encryption functions, i.e. permutations of binary n-bit vectors, high structural complexity.
The rotations that are dependent on data can be accomplished rapidly in software and hardware. Joining with mathematics operations like addition. These combining operations are very active against linear cryptanalysis.

c) The Proposed algorithm is aimed to use a full list of “strong operations” supported in modern computers to attain well security, high speed, and execution flexibility. Proposal algorithm is used primitive operations (add, subtract, multiply, exclusive-or, and data-dependent rotate). The proposal algorithm is resistance against linear and differential attacks by using four key dependent (S-box) tables of 255 each entry is 32-bit.

Example

Let the X is entered to FB function

\[ X = 01100101101101001001101010100111 \]

\[ X \text{ in dec} = 170634887 \]

\( a = 01100101 \) in decimal equal to \( 101 \)

\( b = 10110100 \) in decimal equal to \( 180 \)

\( c = 10011010 \) in decimal equal to \( 145 \)

\( d = 10100111 \) in decimal equal to \( 167 \)

**Figure 6.** The Proposed Design of FB

**Figure 7.** The Extended of FB Function
After performing the following formula:

\[
FB(X) = ((Outa + Outb \mod 2^{32}) \text{ XOR } Outc) + Outd \mod 2^{32}.
\]

\[
FB(X) = 3874430971
\]

\[
FB(X) = 11100110110110001111111111011
\]

\[
FB(X) = 111001101101100011111111111111011
\]

### 2.2 Subkeys

The range of values to be taken by the key has become large. A large key space is necessary to prevent exhaustive search for a key. The proposed system still uses the same key generation process because it is designed to keep the entire key entropy and to distribute this entropy uniformly across the subkey. It is also designed to randomly the permissible subkey set throughout the possible domain of possible subkey [20].

The number of iterations desired for security may be reliant on key length. Note that with the previous subkey generation procedure, a 16-iteration algorithm cannot take a key lengthier than 448 bits (56 bytes). In the proposed algorithm the numbers of iterations for each \( F \) function are 4-iterations; and the numbers of required subkeys are 10 consequently, the total numbers of iterations are 40 and then proposed 40-iteration algorithm does not take a key lengthier than 3200 bits (400 bytes). The improved algorithm uses:

1. The \( P \)-array of 100 32-bits subkeys:
   \[ K_1, K_2, \ldots, K_{100}. \]
2. There is four 8-bit \( S \)-boxes with 255 entries:
   \[ S_{0,1}, S_{0,2}, \ldots S_{0,255}. \]
   \[ S_{1,1}, S_{1,2}, \ldots S_{1,255}. \]
   \[ S_{2,1}, S_{2,2}, \ldots S_{2,255}. \]
   \[ S_{3,1}, S_{0,2}, \ldots S_{3,255}. \]

Data encryption or decryption required the \( P \)-array and \( S \)-boxes are precomputed. The same procedure, which is used in the previous Blowfish algorithm, is used in this work to generate these subkeys.

### 3. Experimental Results

The experiments are conducted on different standard images with different characteristics such as more details and large areas with the same color. These color images of size 256×256 are ‘Lena’, ‘A’, ‘Nike’, ‘Baboon’, ‘Duck’ and ‘Airplane’ as shown in Figure 13. Figure 16 illustrates the original tests images with corresponding permuted and encrypted images by proposed algorithm. As it noticed that the encrypted image is similar to noise image, and there is no relationship with the original image. Thus, the encryption effect is good. While Figure 14 shows the ‘Lena’, ‘A’ and ‘Nike’ test images after encrypted them with traditional Blowfish algorithm. It can be seen that the Blowfish algorithm is not suitable for image encrypting although it an excellent symmetric cryptosystem the reason for this is that the image data is huge and contains more redundancy than the text data.

---

**Figure 8.** Test Images.
3.1 Key Space

The large key space is essential to avoid comprehensive search for a key (Solve the problem of discovery the exact key value by trying potential values until the correct key is found). The proposed system employed Quadratic map which is used two independent variables \( x_0 \) and \( a \). As a result, the key space is \( \{X_0, a\} \). Since \( X_0 \) and \( a \) are double precision numbers, the total number of different values for \( X_0 \) and \( a \) is more than \( 10^{14} \). The used secret keys are six initial conditions \( X_0, X_0', X_1, X_1', X_2, \text{ and } X_2' \) with six parameters \( a_1, a_1', a_2, a_2', a_3 \text{ and } a_3 \). So, the key space is larger than \((10^{14})^{12} = 10^{168} \approx 2^{558}\). The key space of enhanced blowfish algorithm is \( 2^{400} \) the total key space of proposed system is \( 2^{958} \). The key space between the used algorithm and other similar encryption algorithms is compared as shown in Table 1. It is clear that utilized algorithm’s key space size is larger than that of most similar algorithms. Key space for our improved encryption scheme is decently large.

| Encryption Algorithm | Key Space |
|----------------------|-----------|
| Zhu et al. [22]      | \( 2^{339} \) |
| Wang et al [23]      | \( 2^{149} \) |
| Guesmi et al. [24]   | \( 2^{356} \) |
| Li et al. [25]       | \( 2^{299} \) |
| Li et al. [26]       | \( 2^{375} \) |
| Curiac et al. [27]   | \( 2^{128} \) |
| Curiac et al. [28]   | \( 2^{357} \) |
| Proposed algorithm   | \( 2^{958} \) |

3.2 Matching Ciphertext Attack

The 320-bit block size is required to \( 2^{320} \) ciphertexts and this makes the suggested system resistant to corresponding ciphertext attack. Then after the blocks are encrypted, equal ciphertexts can be predictable and information about plaintext is leaked. In the traditional blowfish algorithm with 64-bit block size is required to \( 2^{64} \) ciphertexts [29].

3.3 Memory Requirement

One of the aims of the enhanced Blowfish algorithm is to reduce the memory requirement without compromising security. Hence, the size of S-boxes of Blowfish is reduced. Table 2. illustrates the memory requirement for the S-box to the traditional Blowfish algorithm and enhanced algorithm.

Figure 8: Experiment results. (a) Original images. (b) Encrypted images by Blowfish. (c) Encrypted image by proposed system.
Table 2. Comparison of memory requirements

| Algorithm          | Block Size in bits | Memory requirements in bytes | Iteration numbers |
|--------------------|--------------------|-----------------------------|-------------------|
| Traditional Blowfish | 64                 | 4096 for S-boxes 72 for P   | 521               |
|                    |                    | Total: 4168                 |                   |
| Proposed Algorithm | 320                | 1024 for S-boxes 400 for K  | 178               |
|                    |                    | Total: 1424                 |                   |

3.4 Statistical Analysis

In this section the statistical analyses are conducted on test images represented by information entropy, histogram analysis, and correlation analysis as explained in next subsections.

3.4.1 Histogram Analysis

The histogram can reflect the accurate representation of pixel value distribution. For desirable cryptographic results, the histogram of the encryption image is always uniform. Figure 17 is the original test images, Figure 15 is the histograms of ‘lena’, ‘A’ and ‘nike’ test images, Figure 16 is the histograms of encrypted images by Blowfish algorithm while Figure 17 show the histograms of encrypted images by proposed algorithm. As seen that the experimental results are distributed uniformly, which are totally different from Airfield’s. Therefore, the proposed algorithm has effective resistance from statistical attack.

Figure 9. Histogram Results (a) Original test images. (b) Histogram of R band. (c) Histogram of G band. (d) Histogram of B band.
Figure 10: Histogram of Encrypted images by Blowfish. (a) Encrypted images. (b) Histogram of encrypted R band. (c) Histogram of encrypted G. (d) Histogram of encrypted B band.

Figure 11: Histogram of Encrypted images by proposed system. (a) Encrypted images. (b) Histogram of encrypted R band. (c) Histogram of encrypted G. (d) Histogram of encrypted B band.

3.4.2 Entropy Analysis

Entropy is defined as measure of image information content, which is meant the average number of bits of the gray levels of an image. An increasing in the value of entropy means an increasing in the confusion of information delivered by the image. For discrete 2D images the information entropy $E$ is evaluated using equation (2):

$$E = -\sum_{i=0}^{n} p_i \log_2(p_i)$$

Where, $p_i$ is a gray value probability. When the probability of distributing information is equal to the encrypted image, that is, the probability of each pixel value of [0, 255] is 1/256, maximum entropy is 8 bits. The more confusing information provided by the image will be given higher entropy. The information entropy of test images is listed in Table 3 and the information entropy of the ciphered images attained by Blowfish algorithm is listed too. Table 4 lists the information entropy of proposed algorithm for test images. Note that the entropy of the encrypted image information for all test images is very nearby to 8 bits and that the suggested algorithm has a greater dominance.

| Table 3. Entropy of original images and its encrypted images by Blowfish |
|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| **Image** | **Original image** | **Encryption image** | **Original image** | **Encryption image** | **Original image** | **Encryption image** | **Original image** | **Encryption image** |
| | R | G | B | R | G | B | R | G | B | R | G | B | R | G | B |
| Lena | 7.2865 | 7.5592 | 7.0527 | 7.2871 | 7.9959 | 7.2851 | | | | | | | | |
| A | 1.1608 | 1.1608 | 1.1608 | 5.8673 | 5.9045 | 5.9437 | | | | | | | | |
| Nike | 1.1818 | 1.0344 | 1.0159 | 4.4781 | 5.9453 | 4.5771 | | | | | | | | |
| Baboon | 7.6202 | 7.3139 | 7.6277 | 7.9989 | 7.9973 | 7.6679 | | | | | | | | |
| Duck | 6.4327 | 6.1336 | 6.7851 | 4.3545 | 6.5932 | 4.4239 | | | | | | | | |
| Peppers | 7.3444 | 7.5501 | 7.1173 | 7.3675 | 7.99732 | 7.3551 | | | | | | | | |

| Table 4. Entropy of original images and its encrypted images by proposed system |
|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| **Image** | **Original image** | **Encryption image** | **Original image** | **Encryption image** | **Original image** | **Encryption image** | **Original image** | **Encryption image** |
| | R | G | B | R | G | B | R | G | B | R | G | B | R | G | B |
| Lena | 7.2865 | 7.5592 | 7.0527 | 7.9980 | 7.9980 | 7.9981 | | | | | | | | |
| A | 1.1608 | 1.1608 | 1.1608 | 7.9978 | 7.9981 | 7.9980 | | | | | | | | |
| Nike | 1.1818 | 1.0344 | 1.0159 | 7.9979 | 7.9978 | 7.9978 | | | | | | | | |
| Baboon | 7.6202 | 7.3139 | 7.6277 | 7.9980 | 7.9979 | 7.9978 | | | | | | | | |

13
3.4.3 Correlation Analysis

To increase the level of security in the image we must reduce the correlation between adjacent pixels of the original image. It is noticed that a slight difference in the value of gray in the larger area of the original image. Thus, encryption must have a strong effect on the image. As a test, the correlation coefficients of all adjacent pixels in the three directions, including the vertical, horizontal and diagonal directions are calculated using Equation (3):

\[ r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}} \times \sqrt{D(y)} \]  \hspace{1cm} (3)

Where \( \cos(x,y) = \frac{1}{N} \sum_{i=0}^{N} (x_i - E(x))(y_i - E(y)) \), \( D(x) = \frac{1}{N} \sum_{i=0}^{N} x_i^2 - E(x)^2 \), \( E(x) = \frac{1}{N} x_i \).

The two adjacent pixel values from four directions are represented by \( x \), \( y \), and \( N \) is image pixels’ number.

The correlation distribution map for R, G, and B bands in horizontal, vertical and diagonal directions for original ‘lena’, ‘A’ and ‘nike’ are depicted in Figure 18. The encrypted images by Blowfish and encrypted images by proposed system are drawn and shown in Figure 19 and Figure 20 respectively. Note that in the original images there is a high correlation between adjacent pixels, viewing a linear relationship, this correlation is critically weakened, and for ciphered images viewing a robust randomness. This indicates that the effectiveness of image encryption is good and higher security level.

| Duck    | 6.4327 | 6.1336 | 6.7851 | 7.9982 | 7.9982 | 7.9981 |
|---------|--------|--------|--------|--------|--------|--------|
| Peppers | 7.3444 | 7.5501 | 7.1173 | 7.9981 | 7.9981 | 7.9980 |

**Figure 12.** Correlation coefficients of original test images. (a) Horizontal correlation. (b) Vertical correlation. (c) Diagonal correlation.
Figure 13. Correlation coefficients of encrypted images by Blowfish. (a) Horizontal correlation. (b) Vertical correlation. (c) Diagonal correlation.

Figure 14. Correlation coefficients of encrypted images by proposed system. (a) Horizontal correlation. (b) Vertical correlation. (c) Diagonal correlation.

The proposed method is compared with other methods, while using entropy correlation analysis for the “Lena” image of size 256 × 256 in Table (5).

Table 5. Performance comparisons with other methods

| Measure         | Li et al. [30] | Ahmad and Wang [31] | Zhang and Xiao [32] | Xu et al. [33] | Wang et al. [34] | Hussain et al. [35] | Blowfish [17] | Proposed |
|-----------------|----------------|---------------------|---------------------|----------------|------------------|---------------------|----------------|----------|
| Horizontal      | 0.0327         | 0.9407              | 0.0018              | −0.0230        | 0.0020           | −0.0067             | 0.0064         | −0.0031  |
| Vertical        | 0.0219         | −0.0273             | 0.0011              | 0.0019         | −0.0007          | −0.0137             | 0.0017         | 0.0072   |
| Diagonal        | 0.0180         | −0.0142             | −0.0012             | −0.0034        | −0.0004          | −0.0563             | −0.0048        | −0.0025  |
| Entropy         | 7.9993         | n/a                 | 7.9994              | 7.9974         | 7.9970           | n/a                 | 7.9974         | 7.9981   |

From the observation of Table 5, the Correlation Coefficients of the encrypted ‘Lena’ image using the proposed algorithm are closer to zero than original Blowfish and other researchers, indicating that the encrypted image pixels using the proposed algorithm are highly uncorrelated and cannot predict each other which mean that the proposed algorithm is more secure.

3.4.4 NPCR and UACI Analysis

NPCR and UACI tests, measures the ability of cryptographic system to resist the differential attack. The results of NPCR and UACI tests in Table 6. When the NPCR and UACI of the ciphertext are greater than 99.6% and 33.46%, respectively [36], it indicates that the algorithm has good security compared with traditional Blowfish algorithm and thus the values of the proposed algorithm are closer to the theoretical value than the original Blowfish. Hence, the proposed algorithm is powerfully able to resist differential attacks.
4. Conclusions

The proposed algorithm is 320-bit Blowfish-like block cipher, where cascaded design of composition for $F$-functions is used instead of rounds. The key can be any length up to 400 bytes. The design philosophy of proposed algorithm depends on mixing operation from different algebraic group: XOR, addition, and multiplication. The main aim of proposed algorithm is reduced memory requirement without compromising security. The proposed algorithm is a fast and secure symmetric-key block cipher with a cascaded structure. It offers much improved security/performance over traditional blowfish cipher to gain advantage of the powerful operations reinforced in today’s computers. Because of the low memory requirement, it may be easily to implement on smart cards or other devices with restricted memory.

5. References

[1] Alireza Jolfaei and Abdolrasoul Mirghadri, Image Encryption Using Chaos and Block Cipher, Computer and Information Science, Vol. 4, No. 1; January 2011.
[2] Narendra K Pareek . Design and Analysis of a Novel Digital Encryption Scheme. International Journal of Network Security and Its Application 2012; 4(2): 95-108.
[3] Frank Dachselt ,Wolfgang Schwarz.,: Chaos And Cryptography. IEEE Transactions on Circuits And Systems—I: Fundamental Theory And Applications, Vol. 48, PP. 1498-1501 (2001)
[4] G. A. Sathishkumar, K. Bhoopathy bagan, N. Srirraam, “Image Encryption Based on Diffusion and Multiple Chaotic Maps, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.
[5] Bora, S., Sen, P., Pradhan, C., Novel color image encryption technique using blowfish and cross chaos map. In: IEEE ICCSP 2015 Conference (2015).
[6] L. M. Jawad and G. Sulong, “Chaotic map embeded blowfish algorithm for security enhancement of colour image encryption,” Nonlinear Dynamics, vol. 81, no. 4, pp. 1–15, 2015.
[7] S. N. Gowda, “Using blowfish encryption to enhance security feature of an image,” in 2016 6th International Conference on Information Communication and Management (ICICM), IEEE, 2016, pp. 126–129.
[8] B. Shamina Ross and V. Josephraj, “Performance Enhancement of Blowfish Encryption Using RK-Blowfish Technique”, International Journal of Applied Engineering Research, Vol. 12, No 2, pp. 9236-9244, 2017.
[9] Romani Patel, KrunalPanchal. 2017, Secure Image Encryption Technique Using Blowfish And Chaos, IJARIIE, 3, 2, 4877-4882.
[10] K. Kanagalakshm, M. Mekala. Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key. International Journal of Computer Applications, 146, 5., pp.1-12, 2016.

[11] Zhu, S.; Zhu, C.; Wang, W. A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256. Entropy 2018, 20, 716, 1-18.

[12] Linqing Huang, Shuting Cai, Mingqing Xiao, Xiaoming Xiong. A Simple Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion. Entropy 2018, 20, 535, 1-20.

[13] X. Zhang and X. Wang, “Remote-sensing image encryption algorithm using the advanced encryption standard,” Appl. Sci., vol. 8, no. 3, pp. 1540–1552, 2018.

[14] Ashwaq T. Hashim, Yossra H. Ali, Performance Enhancement of Image Encryption by Using BK-Cube Network Design. Journal of Engineering and Applied Sciences, 13, 18, 7708-7715, 2018

[15] Chunhu Li, Guangchun Luo, and Chunbao Li. An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map. International Journal of Network Security, Vol.21, No.1,22-29, Jan. 2019.

[16] Priya Ramasamy, Vidhyaapriya Ranganathan, Seifedine Kadry, Robertas Damaševicius and Tomas Blažauskas, An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map. Entropy 2019, 21, 656, 1-17.

[17] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption,” Cambridge Security Workshop Proceedings, Springer- Verlag, December 1993, 191-204.

[18] Karthikeyan Bhargavanand Gaëtan Leurent. 2016. On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and Open VPN. In CCS.

[19] J GnuPG Frequently Asked Questions”. Archived from the original on 2017-12-21. Retrieved 2018-01-26. Blowfish should not be used to encrypt files larger than 4Gb in size, but Twofish has no such restrictions

[20] Schneier B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In: Anderson R. (eds) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol 809. Springer, Berlin, Heidelberg.

[21] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, “The RC6TM Block Cipher,” First Advanced Encryption Standard (AES) Conference, Ventura, CA, 1998.

[22] Shuqin Zhu , Congxu Zhu and Wenhong Wang, “A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256”, Entropy, Vol. 20, Issue.716, pp.1-18, 2018. doi:10.3390/e20090716.

[23] Wang, X.; Zhu, X.; Wu, X.; Zhang, Y. Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Opt. Lasers Eng. 2017, 107, 370–379.

[24] Guesmi, R.; Farah, M.A.B.; Kachouri, A.; Samet, M. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm sha-2. Nonlinear Dyn. 2016, 83, 1123–1136.

[25] Li, S.; Chen, G.; Mou, X. On the dynamical degradation of digital piecewise linear chaotic maps. Int. J.Bifurc. Chaos 2005, 15, 3119–3151.

[26] Li, S.; Chen, G.; Wong, K.-W.; Mou, X.; Cai, Y. Baptista-type chaotic cryptosystems: Problems and countermeasures. Phys. Lett. A 2004, 332, 368–375.

[27] Curiaic, D.-I.; Volosencu, C. Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest. Math. Probl. Eng. 2012, 2012, 1-18.

[28] Curiaic, D.I.; Iercan, D.; Dranga, O.; Dragan, F.; Banias, O. Chaos-Based Cryptography: End of the Road? In Proceedings of the International Conference on Emerging Security Information, System and Technologies, Valencia, Spain, 14–20 October 2007; pp. 71-76.

[29] Ross Anderson, Eli Biham, and Lars Knudsen, “Serpent: A Proposal for the Advanced Encryption Standard”, An Internet Survey, 2000.
[30] Li, Y., Li, X., Jin, X.; Zhao, G., Ge, S.; Tian, Y & Wang, Z. (2015). An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map. In Applications and Techniques in Information Security; Springer: Berlin/Heidelberg, Germany, 3–13.

[31] Ahmad, J. & Hwang, S.O. (2016). A secure image encryption scheme based on chaotic maps and affine transformation. Multimed. Tools Appl., 75, 13951–13976.

[32] Zhang, Y. & Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun. Nonlinear Sci. Numer. Simul., 19, 74–82.

[33] Xu, L., Li, Z., Li, J. & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. Opt. Lasers Eng., 78, 17–25. Wang, X. Y., Zhang, Y. Q. & Bao, X. M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. Opt. Lasers Eng., 73, 53–61.

[34] Wang, X. Y., Zhang, Y. Q. & Bao, X. M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. Opt. Lasers Eng., 73, 53–61.

[35] Hussain, I., Shah, T. & Gondal, M.A. (2012). Image encryption algorithm based on PGL (2, GF (28)) S-boxes and TD-ERCS chaotic sequence. Nonlinear Dyn., 70, 181–187.

[36] Chen Liu, Chenghai Li, Fangzheng Zhao, Zijie Zhao, and Hongyi Qiao "Image encryption algorithm based on modified SC-Hopfield", Proc. SPIE 11179, Eleventh International Conference on Digital Image Processing (ICDIP 2019), 1117912 (14 August 2019).