Multimedia Tools and Applications (2023) 82:31575–31589
https://doi.org/10.1007/s11042-023-15105-6

Image encryption using the new two-dimensional Beta chaotic map

Najet Elkhalil[1] · Youssouf Cheikh Weddy[1] · Ridha Ejbali[1]

Received: 24 May 2022 / Revised: 29 September 2022 / Accepted: 12 March 2023 /
Published online: 21 March 2023

Abstract

To further improve the security of the image encryption methods based on chaotic maps, we created a new two-dimensional chaotic map called two Dimensional Beta Chaotic Map(2D-BCM) driven from the one-dimensional Beta chaotic map(1D-BCM). This paper describes a new image encryption approach based on 2D-BCM. The new 2D-BCM is used to produce chaotic sequences. These sequences were used to create the encryption key. The proposed algorithm is composed of three main steps: Permutation, diffusion, and substitution. For the proposed scheme, the generally used metrics of security, and sensitivity to initial conditions are effectively determined with the help of a selection of standard simulation results. In comparison to prior schemes, the obtained results of various types of security analysis show that the newly created 2D-BCM has high sensitivity and security.

Keywords Image encryption · 2D Beta chaotic map · Beta chaotic map · Security

1 Introduction

Information security has become a major concern in to- day's world since our lives depend on technology and information transmission. Images as one of the most transmitted data are the interest of many researchers.

Among different image security metrics like Watermark [30], and Steganography [26], image encryption is a straight- forward one with concerns in encrypting an image to an unrecognized

✉ Najet Elkhalil
najet.elkhalil@isimg.tn

Youssouf Cheikh Weddy
youssefindeh8@gmail.com

Ridha Ejbali
ridha_ejbali@ieee.org

[1] Research Team in Intelligent Machines, National Engineering School of Gabes B.P.W, 6072 Gabes, Tunisia

one. The rapid advancement of chaos theory and its excellent properties present an opportunity for researchers to improve several traditional encryption schemes and build new ones [4, 18, 20, 21, 29]. R. Matthews [23] was the first who presents and published the chaotic map encryption. Following that, many researchers developed image encryption techniques based on chaotic maps. Beginning with the one-dimensional chaotic maps to the n-dimensional chaotic maps our related work is illustrated as follows: Authors in [9] proposed an encryption-compression algorithm. The encryption is done with the Chiricov standard map and the compression with the SPIHIT coding.. Zahmoul et all in [24] proposed a new one-dimensional chaotic map called Beta chaotic map(1D-BCM) based on the Beta equation and the Beta wavelet [34]. This map is then used in image encryption. In the same manner as [9] this new map is then used by Elkhalil et all in [7] to build a robust compression-encryption algorithm. Results show the effectiveness of the BCM in the encryption algorithm and also the flexibility of this map to adapt to the compression part. In ref. [27] another type of 1D-BCM called Wide Range Beta Chaotic Map is presented with the lifting wavelet transform and the Latin square to prove for more time its strengths.

Belazi et all in [1] suggested a new image encryption permutation substitution algorithm based on a chaotic map. Also, Elghandour et all proposed in [6] a new encryption algorithm based on a two-dimensional piecewise smooth nonlinear chaotic map. Their results have proved the high-level protection of images. Hua and Zhou proposed in [12] new two- dimensional Sine Logistic modulation map (2D-SLMM) and used this map in the image encryption process. In this scheme, the authors designed a mechanism to add random values in the images to increase the encryption probability. According to the testing results, the suggested technique can protect images with a good level of security and low time complexity. Another work was reported by Sharm in [28] using a new 2D chaotic map-based encryption technique. The idea behind the new 2D chaotic map is to split the outputs of a 2D logistic map into two distinct 1D logistic maps. Gao in [8] proposed a 2D hyperchaotic map which is derived from 1D-chaotic map. Results show that the 2D hyperchaotic map has more complexity, and randomness than a 1D hyperchaotic map. Moreover, the security analysis has good results. In [22] authors proposed a new image encryption scheme based on three-dimensional Lorenz chaotic system. A 3D chaotic economic map was used in [15]. In [17] authors proposed an optical encryption scheme based on hybrid 3D chaotic maps and discrete cosine transform. The original images was converted to an indexed formats using their color maps. The 3D-logistic chaotic map is used to generate a chaotic sequence (key stream) that will be used to shuffle the indexed images. The encrypted image is obtained after separating the amplitude and phase part of the signal. The experimental results prove that the proposed scheme is resistant to the chosen plain-text attacks.

Authors in [5] proposed a hybrid chaos image encryption scheme. Two-dimensional ecological chaotic map, Free and Lawton (BFL) map was combined with logistic map and Chebyshev map to generate a pseudo-random sequence for image encryption key. Results show that the proposed scheme has good immunity against several cryptography attacks.

As can be observed, seemingly little changes in the mathematical formulation result in considerably innovative and successful encryption algorithms [2, 3, 10, 11, 13, 32, 33]. The current work was inspired by the work of Zahmoul et all in [25] and Wu et all in [31].

2 Our contribution

To further ameliorate the performance of the 1D Beta chaotic map, we create new 2D Beta chaotic map based on 1D Beta chaotic map function.

Our new map has a large range of bifurcation parameters, strong chaotic behavior and high number of parameters.

Our map is used to generate pseudo-random sequences. Those chaotic sequences are used to generate the encryption key, furthermore, they were used in the permutation and substitution process.

This paper is organized into the following sections. Section 2: Displays the review of 2D chaotic maps. Section 3: Devoted to introducing the new 2D-BCM; the mathematical definition and the bifurcation diagram. The encryption algorithm is detailed in Section 4. Section 5: details the security analysis and results and Section 6: Gives a general conclusion.

3 Review of 2D chaotic maps

The 2D chaotic maps lead to 2D iterate $xi + 1$, $yi + 1$ from the previous xi and y_i. Here, we will present some of the proposed 2D chaotic maps.

3.1 2D logistic map

The 2D logistic map (2D-LM) was suggested by Wu et all in [31] and used for image encryption. Security analysis results reflect its performance and efficacity. The 2D-LM is defined as

$$x_{i+1} = r\left(3_{y_i} + 1\right)x_i(1 - x_i) \tag{1}$$

$$y_{i+1} = r\left(3_{x_{i+1}} + 1\right)y_i(1 - y_i) \tag{2}$$

3.2 2D sine logistic modulation map

The 2D Sine Logistic Modulation Map (2D-SLMM) proposed by Hua et all in [13] is defined as follows:

$$xi + 1 = \mu[sin(\pi yi) + 3]xi(1 - xi) \tag{3}$$

$$yi + 1 = \mu[sin(\pi xi + 1) + 3]yi(1 - yi) \tag{4}$$

4 New 2D Beta chaotic

Derived from the 1D Beta chaotic map proposed by Zahmoul et all in [24, 31] and defined as follow:

$$x_{n+1} = k \times Beta\ (yn; x1, x2, p, q) \tag{5}$$

where

$$p = b_1 + c_1 \times a \tag{6}$$

$$q = b_2 + c_2 \times a \tag{7}$$

b_1,c_1,b_2 and c_2 adequately chosen constants.

a: bifurcation parameter.

k: amplitude control parameter.

We created a new 2D Beta chaotic map. The 2D-BCM has more chaotic behavior and large bifurcation diagram than the 1D-BCM.

4.1 Mathematical definition

The mathematical definition of our map is as follows:

$$x_n + 1 = k \times Beta\ \left(y_{n+1}; x1, x2, p, q\right) \tag{8}$$

$$y_n + 1 = k \times Beta\ (xn; y1, y2, p, q) \tag{9}$$

where

$$p = b1 + c1 \times a \tag{10}$$

$$q = b2 + c2 \times a \tag{11}$$

b_1,c_1,b_2 and c_2 adequately chosen constants.

a: bifurcation parameter.k: amplitude control parameter.

4.2 Bifurcation diagram of the 2D-BCM

A bifurcation diagram illustrates a qualitative change in dynamics as a result of a simple change in one of parameters. The dotted line in the bifurcation diagram generally relates to the system’s chaotic behavior; the solid line, on the other hand, indicates that the system’s behavior has been adjusted to be periodic [16]. Figure 1 shows the different 2D Beta Chaotic maps. Our maps characterized by strong chaotic behavior, better pseudo random sequences, wide range of bifurcation parameters, and a large number of parameters.

As result, encryption process become more efficient and could stand up to most attacks.

4.3 The Lyapunov exponent

Lyapunov exponent represents a quantitative measure of chaos. It is commonly used to determine whether the given system has a chaotic behavior or not.

The Lyapunov exponent of the Beta chaotic map is positive as indicated in ref. [27]. Our present work is based on the Beta map, thus the 2D Beta chaotic map is an extended version of

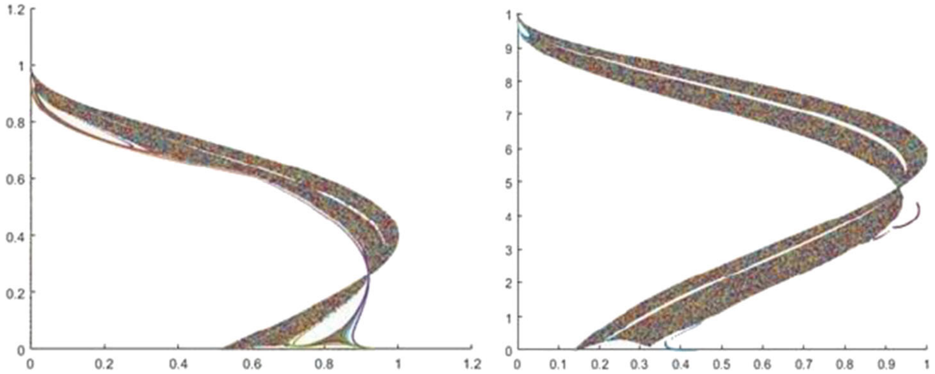

Fig. 1 Different shapes of the 2D-BCM

1D chaotic map. Thus we can conclude that the Lyapunov exponent of 2D Beta chaotic map has a large number of positive values.

5 Proposed encryption algorithm

Step 1: Resizing the plain text image to a square dimension.

Step 2: We employed the 2D-BCM with its parameters and initial values to create the encryption key. Weused the initial values ×0, y0, and k to generate a sufficiently long chaotic sequence, whose length equals to the number of pixels in the plaintext image P. The encryption key control the pseudo random sequences generated from the 2D-BCM. Xseq and Yseq be the 2D- BCM x and y coordinate sequences, respectively.

Step 3: The rows and columns of the plaintext image are now shuffled using the Beta chaotic maps' generated sequences. We sorted the Xseq and the Yseq in a matrix form, to obtain 2 matrices M1 and M2. Per- mute the plain text images pixels within columns, using the position of M1 elements. After the column permutation, we permute the resulting matrix using the M2 rows positions.

Step 4: The substitution step is done, by first: dividing the resulting matrix of the permutation step into four equal-sized blocks B. After that, each 4*4 block B will be changed using the functions below:

$$f_N(d) = T(d) mod G \tag{12}$$

$$R(d) = T\left\lfloor \left(\sqrt{d}\right) \right\rfloor \text{modG} \tag{13}$$

$$f_s(d) = T\left(d^2\right) mod G \tag{14}$$

$$f_D(d) = T(2d) mod G \tag{15}$$

And the matrix function is given below:

$$W=\begin{bmatrix} f_N(B_{1,1}) & f_R(B_{1,2}) & f_S(B_{1,3}) & f_D\ (B_{1,4}) \\ f_R(B_{2,1}) & f_S(B_{2,2}) & f_D(B_{2.3}) & f_N(B_{2.4}) \\ f_N(B_{3.1}) & f_D(B_{3.2}) & f_N(B_{3.3}) & f_R(B_{3.4}) \\ f_D(B_{4.1}) & f_N(B_{4.2}) & f_R(B_{4.3}) & f_S(B_{4.4}) \end{bmatrix} \tag{16}$$

Function T: is a truncation of a decimal to form an integer for every number of the resulting matrix W. G: represents the image type. For 8-bit gray images G = 256 and for the binary images G = 2.

Here we got a new random integer matrix I. So, we can now determine the encrypted image C using the following equation:

$$C=(P+I)mod\ G \tag{17}$$

And the decrypted image P by:

$$P=(C{-}I)mod \tag{18}$$

Step 5: The last step in our algorithm is the diffusion stage. In this stage we aim to eliminate the redundancy in the statics and information contained in the original image in the ciphered one. It is done by changing each pixel in the original image over the finite field GF(28). Figure 2 illustrates the steps mentioned above, and Fig. 3 represents the flowchart of the hole process.

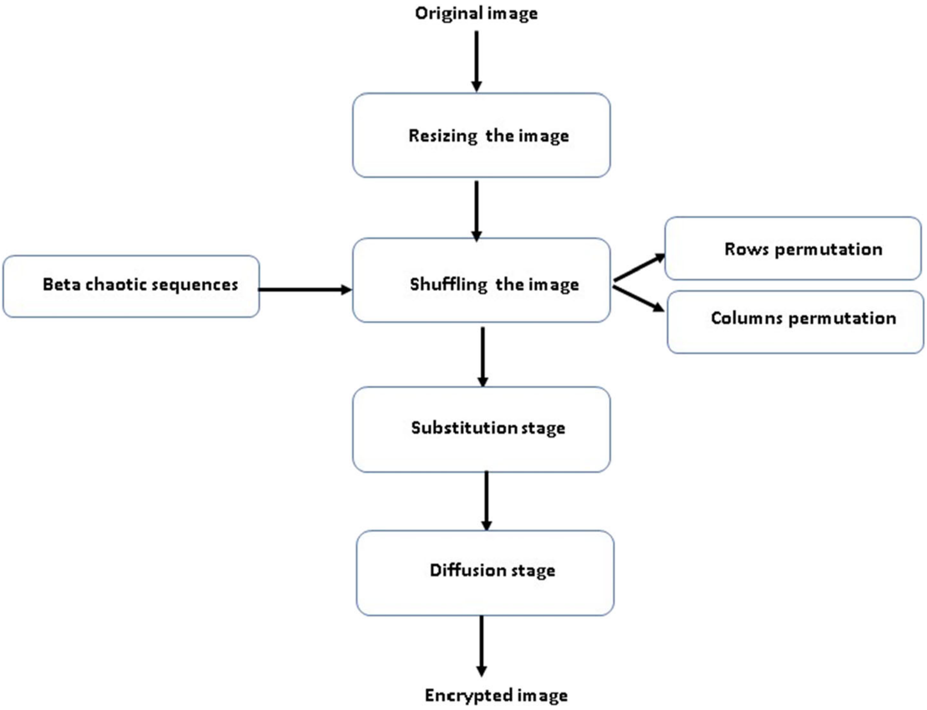

Fig. 2 Detailed Steps of the encryption algorithm

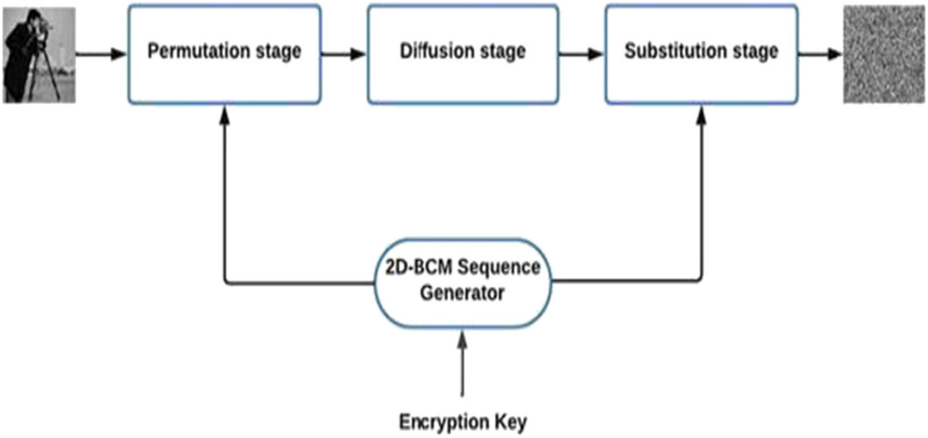

Fig. 3 Diagram of the encryption process

6 Experimentation and results

Noise and data loss can easily affect digital images through transmission over the network and computer storage, which is normally done by changing one or more bits.

Furthermore, an efficient encryption algorithm should be resistant to all known attacks and its performance should not be dependent on the original image or the encryption key. Our experiments were carried out using different images from the USC-SIPI Image Database as plaintext images and various security tests. A comparison is made with different published algorithms. The next paragraphs go over the findings.

6.1 Histogram analysis

Histogram bars for a plain image are uneven, indicating that some information is carried in the plain image [14]. Also, The randomness of pixel values is indicated by the flatness of histogram bars. Thus the encrypted image's histogram bars should be flat in order to resist to differential attack. The histograms of the encrypted images are shown in Fig. 4, whereas the

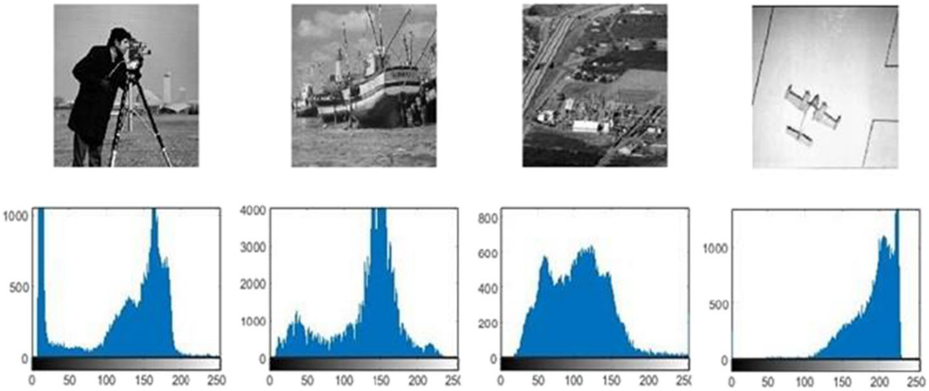

Fig. 4 Respectively from left to right: Encrypted images and their histograms Cameraman, Boat, Chemical plant, Airplane

plain image ones are shown in Fig. 5. Evidently, the encrypted images can be considered random-like images and have no discernible characteristics.

6.2 Information entropy

Information entropy can be used to show the random- ness of the cipher image. It can be calculated as follows:

$$H(S) = \sum_{i=1}^{2^n-1} P(S_i)\log\left(\frac{1}{P(S_i)}\right) \tag{19}$$

Where

2^n: the total states of the information source S_i,
$P\ (S_i)$: the probability of symbol S_i.

The information entropy for the encrypted images using our method is presented in Table 1. Also, a comparison with algorithms in [12, 25, 31] is established in Table 2.

Results prove that the entropy of the encrypted images using our algorithm is extremely near to the theoretical value 8. Our entropy average 7.99% is the closest to the expected one than [5, 12, 25, 31]. As a result, we can conclude that the randomness is achieved and our proposed method is strong against differential attack.

6.3 Sensitivity analysis

In the field of image encryption, sensitivity analysis are crucial metrics. They are often used to test the sensitivity of the plain image and the secret key. A few changes to any one of them results in a nonidentical

Cipher image in the efficient algorithm [8].

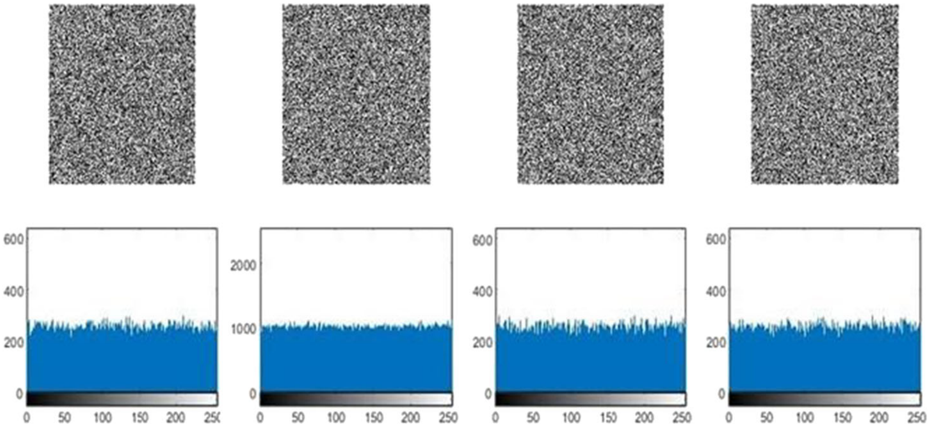

Fig. 5 Respectively from left to right: original images and their histograms: Cameraman, Boat, Chemical plant, Airplane

Table 1 Entropy average of our approach

Image name	Our approach
Airplane	79,998
Airport	79,998
Boat	79,993
Camera man	79,996
Chemical plant	79,972
Clock	79,970
Couple	79,992
Moon surface	79,973
Tank	79,993
Average	799,883

6.3.1 Key sensitivity analysis

Key sensitivity has a significant impact on the security of a cryptosystem. As a result, a single bit variation in the key should result in different ciphered images. As demonstrated in Figs. 6 and 7, the suggested approach demonstrates the encryption key's high sensitivity. It also proves the key sensitivity in consideration of encryption and decryption, where K1,K2 and K3 re different by only one bit.

6.3.2 Plain image sensitivity

The sensitivity test is done by changing the value of one pixel in the original image, after that comparing the encrypted images of the original image with the en crypted images of the modified one. The sensitivity to the plain image will be measured using two metrics. The first one is the Number of Pixels Change rate (NPCR) and the second one is the unified average changing Intensity (UACI).NPCR and UACI are calculated as follows:

$$NPCR \quad = \quad \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{20}$$

Table 2 Entropy average of our approach and algorithm in [12, 25, 31]

image name	our approach	Ref [25]	Ref [31]	Ref [12]	Ref [5]
Airplane	79,998	79,998	79,998	79,954	–
Camera man	79,996	79,972	79,971	79,964	79,991
Chemical plant	79,972	79,971	79,974	79,990	–
Clock	79,970	79,975	79,972	79,956	–
Moon surface	79,973	79,975	79,971	79,954	–
Airport	79,998	79,998	79,998	79,969	79,998
Couple	79,992	79,993	79,992	79,980	–
Tank	79,993	79,994	79,993	79,965	–
Boat	79,993	79,993	79,993	79,965	–
Test pattern	79,998	79,998	79,995	79,984	–
average	79,988	79,986	79,985	79,968	–

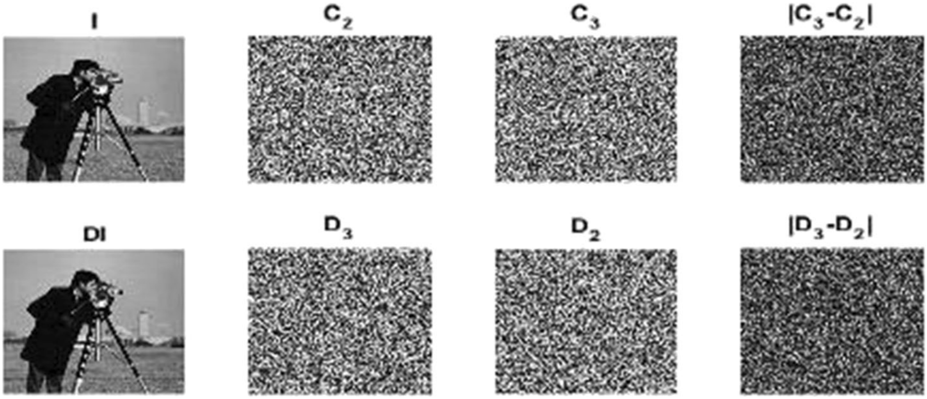

Fig. 6 Key sensitivity results: Encrypted image C2 = Encryption(I,K1),Encrypted image C3 = Encryption(I,K2); Encrypted image difference C3 C2; Decrypted image DI=Decryption(C2,K1); decrypted image D2 = Dec(C2,K2); decrypted image D3 = Decryption(C2,K3); decrypted image difference D3-D2(K1 and K2 are different only in one bit; K2 and K3 are also different only in one bit; and K1 K3)

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100\% \tag{21}$$

Where

$$D(i,j) = \begin{cases} 0 & if \quad C_1(i,j) = C_2(i,j) \\ 1 & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \tag{22}$$

M and N: the height and the width of the original and the cipher images, C1 and C2 are the encrypted images before and after one pixel is modified from the original image, respectively. Tables 3 and 4 rep- resent the NPCR and UACI of the tested images by applying our algorithm and the suggested in literature [11, 19, 25, 28, 31]. Our NPCR and UACI average is about 99.6236%,33.49337%, respectively. For comparison, among all the encryption schemes as

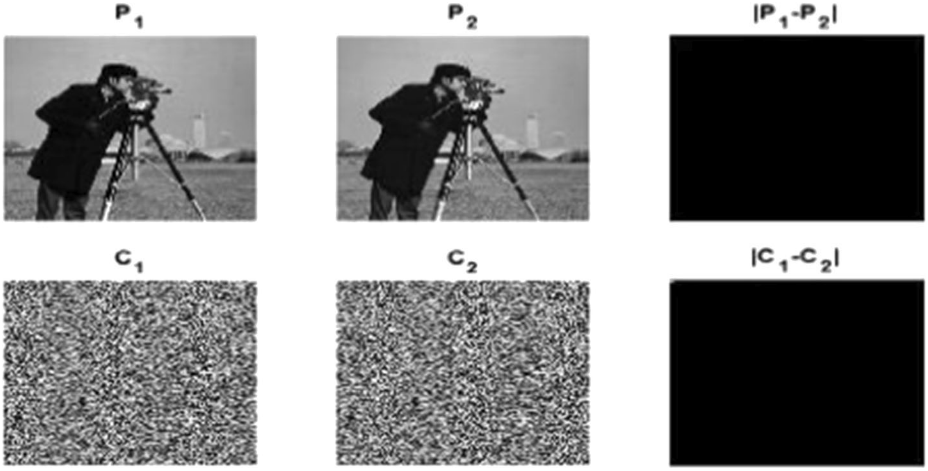

Fig. 7 Number of pixel change rate (NPCR) in the plain and encrypted images of Cameraman

Table 3 NPCR results of our approach and other approaches

image name	our approach	Ref [25]	Ref [31]	Ref [19]	Ref [19]	Ref [11]	Ref [28]
Airplane	99.5987	99.6459	99.5972	99.64	49.8138	99.6244	99.6044
Airport	99.6643	99.5849	99.6005	99.62	99.6163	99.6128	99.6138
Boat.512	99.6261	99.6227	99.6037	99.61	99.6037	99.6154	99.606
Chemical plant	99.6368	99.6200	99.5773	99.62	99.6368	99.6364	99.6124
Clock	99.6063	99.5727	99.6201	99.60	49.828	99.5703	99.6044
Couple	99.6200	99.6185	99.63	99.61	99.6208	99.587	99.6079
Elaine.512	99.6094	99.6292	99.6082	99.6	99.6292	99.6196	99.6079
Moon Surface	99.6735	99.6276	99.5804	99.60	49.8093	99.6064	99.6139
Tank	99.6124	99.6307	99.6117	99.59	49.8096	99.6079	99.5911
Test pattern	99.5880	99.6105	99.6117	99.62	99.6108	99.6072	99.6178
Average	99.6236	99.6150	99.6040	99.611	79.6978	99.6087	99.6080

listed in Tables 3 and 4, our algorithm achieves the expected average of NPCR and UACI (99.6094%, 33.4635%) . Thus, we can conclude that the proposed algorithm is very sensitive to changes in the plain image and that even small changes in the plain image result in completely different cipher images. As a result, the proposed technique can overcome differential attacks.

6.4 The mean square error analysis

The Mean Square Error (MSE) is a metric that de- scribes the difference between the original image and the encrypted one. Pixels are represented by numbers between 0 and 255.

$$MSE = \frac{1}{MN} \sum_{i=1}^{N} \sum_{j=1}^{M} \left[C(i,j) - C^{'}(i,j) \right] \tag{23}$$

M, N: the size of the original or the ciphered image.
C(*i, j*): original image pixel.
C′(*i, j*): encrypted image pixel

Table 4 UACI results of our approach and other approaches

image name	our approach	Ref [25]	Ref [19]	Ref [19]	Ref [11]	Ref [28]
Airplane	33,4593	33,4188	33,24	33,5374	33,4946	33,5922
Boat.512	33,405	33,5137	33,21	33,6291	33,4654	33,3903
Chemical plant	33,5037	33,4291	33,56	34,2965	33,4302	33,4086
Clock	33,3274	33,4444	33,24	17,0621	33,5541	33,4524
Couple	33,4566	33,3615	33,56	33,4267	33,4438	33,2789
Moon Surface	33,3783	33,4408	33,14	16,6687	33,4456	33,4215
Test pattern	33,9225	33,6803	33,43	33,4786	33,4347	33,5022
Average	33,4933	33,4698	33,34	28,0783	33,4669	33,4352

MSE should be as high as possible while encrypting images. A higher MSE value between the original and encrypted image indicates more attack resistance Table 5 shows that the MSE values of our method is better than other in [25, 31].

6.5 Peak signal to noise ratio analysis

Peak Signal to Noise Ratio (PSNR) define the ratio of the noise and the highest achievable power that influences image representation. It is mostly used as a metric for image reconstruction quality. PSNR defined by the following formula:

$$PSNR = 10\log_{10}\left(\frac{Max_I^2}{MSE}\right) \tag{24}$$

where:

MaxI: the highest pixel value of the image I.

A high PSNR value indicates good image quality. To ensure the efficiency of the suggested method, the difference between two images PSNR should be as little as possible. Table 6 shows the difference in PSNR values between the original and encrypted images. Our method yields a lower PSNR than the one calculated in [25, 31]. We conclude that the proposed approach is more resistant to statistical attacks.

6.6 Key space analysis

It is well noun that a good encryption scheme is characterized by a large key space which enhance its immunity to several attacks.

Our encryption key composed of different parameters of the two coordinate x and y, about 512 bit is sufficient enough to overcome the brute force attacks.

Our encryption key is comparable and even better than other state of the art methods. Thus, the key has high immunity against brute force attacks.

7 Real implementation and future work

All Experimental tests and implementations were realized under the same conditions on the same machine, PC HP; an Intel(R) Core-i7–2.5GHz processor, RAM: 6 Go.

Table 5 MSE values of our method and those in [25, 31]

image name	our approach	Ref [25]	Ref [31]
Airplane	10,994	10,988,48	10,990,67
Barbara	34,483	9275,24	8285,23
Boat	30,876	7532,69	7530,09
Cameraman	9558,9	9488,81	9376,41
Chemical plant	7868,98	7792,67	7778,31
Clock	12,251,63	12,220,64	12,211,31
Couple	28,582	7083,14	6955,55
Lena	31,375,74	7694,3	7779,56
Moon surface	6291,13	6252,33	6229,09
Peppers	43,369	8397,1	8345,43
Average	21,565,038	8672,54	8548,165

Table 6 PSNR of encrypted image using our approach and those in [25, 31]

image name	our approach	Ref [25]	Ref [31]	Ref [5]
Airplane	7,72	7,76	7,75	–
Barbara	2,75	8,49	8,98	–
Boat	3,23	9,4	9,4	–
Camera man	8,33	8,39	8,44	8,10
Chemical plant	9,17	9,25	9,26	–
Clock	7,25	7,29	7,3	–
Couple	3,57	9,66	9,74	–
Lena	3,16	9,3	9,26	8,28
Moon surface	10,14	10,2	10,22	–
Peppers	1,76	8,92	8,95	7.58
Average	5708	8866	8,93	

In the future, we hope to take the new 2D-BCM a step further by incorporating it into steganography, watermarking also in other cryptography techniques.

8 Conclusion

In order to improve the results achieved by the one dimensional Beta Chaotic map, we created a new 2 dimensional beta chaotic map. The bifurcation diagram and the sensitivity to initial conditions of our new 2D- BCM indicate that our map have a good chaotic behavior. The 2D-BCM is then used in an image encryption scheme to better prove its efficiency.

The suggested image encryption method adopts the permutation-substitution network structure and a diffusion step. Results obtained for information entropy, histogram analysis, sensitivity analysis, MSE and PSNR prove that the encryption algorithm has successfully been able to prevent various existing cryptography attacks and cryptanalysis techniques.

Acknowledgements The authors would like to acknowledge the financial support of this work by grants from General Direction of Scientific Research (DGRST), Tunisia, under the ARUB program.

Data availability The datasets analyzed during the current study are available In: https://sipi.usc.edu/database/database.php?volume=misc.

Declaration

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent This work does not have any content needing any informed Consent.

Conflict of interest The Authors declares that they do not have conflict of interest.

References

1. Belazi A, Abd El-Latif A, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170. https://doi.org/10.1016/j.sigpro.2016.03.021

2. Cao C, Sun K, Liu W (2017) Signal Process 143. https://doi.org/10.1016/j.sigpro.2017.08.020
3. Chen G, Mao Y, Chui C (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 21:749. https://doi.org/10.1016/j.chaos.2003.12.022
4. Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB (2015) A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun Nonlinear Sci Numer Simul 20:846860. https://doi.org/10.1016/j.cnsns.2014.06.032
5. De S, Bhaumik J, Giri D (2022) A secure image encryption scheme based on three different chaotic maps. Multimed Tools Appl 81:81–5514. https://doi.org/10.1007/s11042-021-11696-0
6. Elghandour A, Salah A, Karawia A (2021) A new cryptographic algorithm via a two-dimensional chaotic map. Ain Shams Eng J 13:101489. https://doi.org/10.1016/j.asej.2021.05.004
7. Elkhalil N, Zahmoul R, Ejbali R, Zaied M (2019) A joint encryption-compression technique for images based on beta chaotic maps and SPIHT coding. ICSEA, p 130
8. Gao X (2021) Opt Laser Technol 142:107252. https://doi.org/10.1016/j.optlastec.2021.107252
9. Hamdi M, Rhouma R, Belghith S (2016) A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map. Signal Process 131:514–526. https://doi.org/10.1016/j.sigpro.2016.09.011
10. Hsiao HI, Lee J (2015) Color image encryption using chaotic nonlinear adaptive filter. Signal Process 117: 281–309. https://doi.org/10.1016/j.sigpro.2015.06.007
11. Hua Z, Zhou Y (2016) Image encryption using 2D Logistic-adjusted-Sine map. Inf Sci 339:237–253. https://doi.org/10.1016/j.ins.2016.01.017
12. Hua Z, Zhou Y, Pun CM, Chen C (2014) Information Sciences 297. https://doi.org/10.1016/j.ins.2014.11.018
13. Hua Z, Zhou Y, Pun CM, Chen C (2014) 2D Sine Logistic modulation map for image encryption. Inf Sci 297:80–94. https://doi.org/10.1016/j.ins.2014.11.018
14. Hussein W, Al-Saidi N, Kadhim H (2018) pp 265–269. https://doi.org/10.1109/SCEE.2018.8684083
15. Karawia A (2019) IET Image Process 13. https://doi.org/10.1049/iet-ipr.2018.5142
16. Kumar V, Girdhar A (2021) A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach. Multimed Tools Appl 80:3749–3773. https://doi.org/10.1007/s11042-020-09854-x
17. Kumar D, Joshi A, Mishra V (2020) Optical and digital double color-image encryption algorithm using 3D chaotic map and 2D-multiple parameter fractional discrete cosine transform. Results Opt 1:100031. https://doi.org/10.1016/j.rio.2020.100031
18. Li C, Luo G, Qin K, Li C (2017) Nonlinear Dyn 87. https://doi.org/10.1007/s11071-016-3030-8
19. Liao X, Lai S, Zhou Q (2010) A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process 90:2714. https://doi.org/10.1016/j.sigpro.2010.03.022
20. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84: 26. https://doi.org/10.1016/j.optlaseng.2016.03.019
21. Malik D, Shah T (2020) Color multiple image encryption scheme based on 3D-chaotic maps. Math Comput Simul 178:646–666. https://doi.org/10.1016/j.matcom.2020.07.007
22. Masood F, Ahmad J, Shah SA, Sajjad S, Jamal SS, Hussain I (2020) A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map. Entropy 22:274. https://doi.org/10.3390/e22030274
23. Matthews R (1989) On the derivation of a “chaotic” encryption algorithm. Cryptologia 13:29–42. https://doi.org/10.1080/0161-118991863745
24. Rim Z, Zaied M (2016) pp 004,052–004,057. https://doi.org/10.1109/SMC.2016.7844867
25. Rim Z, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 96:39. https://doi.org/10.1016/j.optlaseng.2017.04.009
26. Rim Z, Afef A, Ejbali R, Zaied M (2020) Beta Chaotic Map Based Image Steganography, pp 97–104. https://doi.org/10.1007/978-3-030-20005-310
27. Rim Z, Ejbali R, Zaied M (2021) An improved partial image encryption scheme based on lifting wavelet transform, wide range Beta chaotic map and Latin square. Multimed Tools Appl 80:15173–15191. https://doi.org/10.1007/s11042-020-10263-3
28. Sharma M (2020) Image encryption based on a new 2D logistic adjusted logistic map. Multimed Tools Appl 79:355–374. https://doi.org/10.1007/s11042-019-08079-x
29. Sheela S, Kaggere S, Tandur D (2018) Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimed Tools Appl 77:25223–25251. https://doi.org/10.1007/s11042-018-5782-2
30. Souden H, Ejbali R, Zaied M (2019) p 116. https://doi.org/10.1117/12.2523482

31. Wu Y, Yang G, Jin H, Noonan J (2012) Image encryption using the two-dimensional logistic chaotic map. J Electron Imaging 21:3014. https://doi.org/10.1117/1.JEI.21.1.013014
32. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Process 141:109–124. https://doi.org/10.1016/j.sigpro.2017.04.006
33. Yavuz E, Yazc R, Kasapba MC, Yamac E (2016) A chaos-based image encryption algorithm with simple logical functions. Comput Electr Eng 54:471. https://doi.org/10.1016/j.compeleceng.2015.11.008
34. Zaied M, Ben Amar C, Alimi A (2003) International conference on signal, system and design, SSD03, Tunisia 1, 185

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.