Low Detail Image Encryption Algorithm Based on Diffusion and Confusion Using Henon and Baker Chaotic Map

Ensherah Naeem (ensherah_naeem@yahoo.com)
Suez University
Anand B. Joshi
University of Lucknow
Dhanesh Kumar
University of Lucknow
Fathi E. Abd El-Samie
Menoufia University

Research Article

Keywords: Low detail image, Henon chaotic map, Baker chaotic map, Image encryption, Decryption.

Posted Date: January 21st, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1213667/v1

Low detail image encryption algorithm based on diffusion and confusion using Henon and Baker chaotic map

Ensherah A. Naeem[a,1], Anand B. Joshi[b], Dhanesh Kumar[b], Fathi E. Abd El-Samie[c]

[a]*Electrical Department, Faculty of Technology and Education, Suez University, Suez 43527, Egypt*
ensherah_naeem@yahoo.com
[b]*Department of Mathematics and Astronomy, University of Lucknow, India*
dhaneshkumar.lu@gmail.com
[c]*Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt*
fathi_sayed@yahoo.com

Abstract

This paper presents a solution for the security of low detail images in real-time applications over open or unsecured networks. The diffusion and confusion operations are both performed based on Henon and Baker chaotic map. The XOR and permutation operations are used to obtain diffusion and confusion in the algorithm. In the proposed technique, the high detail image is used as a key. The computer simulation results and security analysis are given to ensure the validity and strength of the proposed technique. In the security analysis, we have analyzed key space analysis, cropping attack analysis, noise attack analysis, and differential attack analysis. Some statistical analyses like entropy, histogram, and correlation coefficients are also given to check the strength of the presented technique.

Keywords: Low detail image, Henon chaotic map, Baker chaotic map, Image encryption, Decryption.

1. Introduction

In the present era of information technology, the communication of multimedia data like text data, digital images, audio, and video data, has increased enormously. Sometimes these digital data contain confidential information, so the security of these digital data stored somewhere or communicated through an open and unsecured channel is a challenging job. In this regard, different types of cryptosystems have been proposed since the encryption is admitted as an effective and direct method to keep confidential information secure from hackers, cyber-criminals, or unauthorized users. There are many image encryption technique in literature based on chaotic maps [1–11].

In the field of image encryption, the encryption technique can be divided into three categories: confusion-only, diffusion-only, and combination of both, i.e., confusion-diffusion. Generally, the confusion-based image encryption algorithm is treated as a weak image encryption algorithm. In [12], Li proposed position permutation on two levels: intra-block and inter-block based image encryption algorithm. Anwar and Meghana [13] also proposed a pixel confusion-based image encryption method using the chaotic map. However, the confusion-only encryption techniques are weak to some powerful attacks [14, 15].

For the diffusion-only image encryption algorithm, Zhu [16] proposed a hyper-chaotic map based image encryption algorithm using two rounds of diffusion operation. But, Ozkaynak et al. [17] revealed that the keys of this image encryption technique could be broken with a chosen plaintext attack; also Li et al. [18] examine the security of [16] and get a weakness against known plaintext attack. Ye and Zhou [19] introduced a chaotic map based digital image encryption technique, in which they only employ diffusion operation. Although authors claimed that the technique is resistant against chosen and known plaintext attacks, Yap and Phan [20] introduced both chosen ciphertext and plain-

[1]Corresponding author email address: ensherah_naeem@yahoo.com

text attacks against this technique.

The permutation-substitution or confusion-diffusion was first introduced by Fridrich [21], which is the most useful combination for image encryption. In this proposed technique, the position of pixels is firstly shuffled to reduce the correlation between the adjacent pixels. After that, the values of the pixels are changed one by one in the diffusion process.

Li et al. [22] proposed a hyper chaotic map based image encryption technique. In this technique, a 5D hyperchaotic system is used to generate confusion and diffusion keys. This technique uses both pixel and bit-level confusion operation and diffusion operation is employed to change the pixels value. Also in [23], authors proposed an approach for bit-level permutation in image encryption using a 3D puzzle along with chaos for further diffusion and confusion.

Liu et al. [24] presented an image encryption system based on the 2D Sine iterative chaotic map with an infinite collapse modulation map and a closed-loop modulation coupling. In this technique, the Chaotic shift transform is used for both confusion and diffusion. In [25], Hamza and Titouna proposed an image encryption technique using the Zaslavsky chaotic sequence. The Zaslavsky sequence is used to produce the pseudo-random number and these numbers are used to produce the encryption key of the cryptosystem. In this technique, the image encryption algorithm is based on confusion-diffusion process.

Ping et al. [26] designed confusion and diffusion based image encryption technique using Henon map. For substitution, a two-point diffusion strategy using the Henon map is proposed. In [27], Mishra and Saharan proposed an image encryption technique based on Henon map and 128-bit private key. In this scheme, the confusion operation is executed using a permutation matrix generated by the Henon map.

The rest of the paper is organized as follows. Section 2 discusses the elementary knowledge of the 2D-Henon chaotic map and 2D-Baker chaotic map. Section 3 discusses the proposed low detail image encryption and decryption algorithm. Section 4 presents the numerical simulation of the proposed technique. Section 5 discusses the security analysis. The statistical analysis is discussed in section 6. Finally, the conclusion of the proposed technique is given in section 7.

2. Preliminaries

This section gives some definitions related to the proposed cryptosystem.

2.1. 2D-Henon chaotic map

Chaotic maps have many unique properties such as initial parameter sensitivity, unpredictability, and ergodicity. The 2D-Henon chaotic map [28] is introduced by French mathematician and astronomer M. Henon in 1976. The Henon map defined on a 2D plane is a nonlinear discrete time dynamical system is defined by Eq. 1,

$$\begin{cases} u_{m+1} = 1 - \alpha u_m^2 + v_m, \\ v_{m+1} = \beta u_m, \end{cases} \tag{1}$$

where u, v are the iterated values and the number of iterations are $m = 0, 1, 2, 3, ...$ α and β are two control parameters of the map. The system 1 shows the chaotic behavior for the values $\alpha = 1.4$ and $\beta = 0.3$. Figure 1 displays the chaotic behavior of Eq. 1 in 10000 iterations with initial parameters $u_0 = 0.5$ and $v_0 = 0.6$.

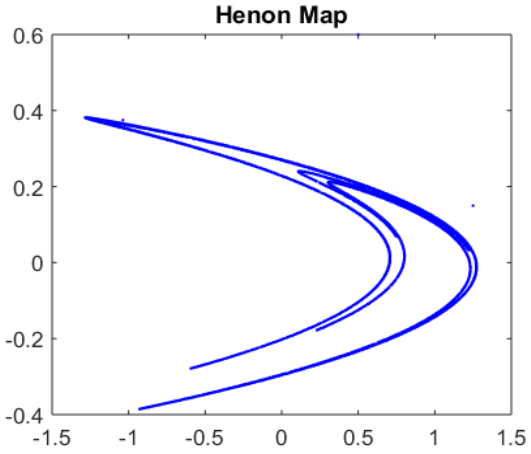


Figure 1: Chaotic behavior of Henon map in 10000 iterations.

2.2. 2D-Baker chaotic map

The Baker chaotic map is the most popular encryption tool in the image processing community. It is a confusion-based tool used in the randomization of the image by changing the pixel positions. It is a 2D map, under it the unit square is mapped into

unit square. The 2D-Baker map [29, 30] is defined by Eqs. 2 and 3,

$$x_{n+1} = \begin{cases} r_1 x_n & \text{if } y_n < \alpha \\ (1 - r_2) + r_2 x_n & \text{if } y_n > \alpha \end{cases} \quad (2)$$

$$y_{n+1} = \begin{cases} \frac{y_n}{\alpha} & \text{if } y_n < \alpha \\ \frac{(y_n - \alpha)}{\beta} & \text{if } y_n > \alpha \end{cases} \quad (3)$$

where $0 < x_n, y_n < 1$ for all $n = \{0, 1, 2, 3, ...\}$, $\beta = 1 - \alpha$ and $r_1 + r_2 \leq 1$. 2D-Baker map generates the random sequences which are used to perform confusion operations in the image pixel.

Fig. 2 depicts the chaotic behavior of Baker map using the first values $x_0 = 0.235$, $y_0 = 0.527$ and control parameters $r_1 = 0.23$, $r_2 = 0.77$, and $\alpha = 0.32$.

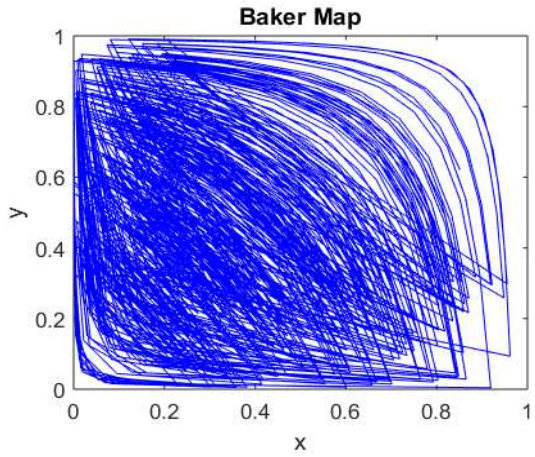


Figure 2: Chaotic behavior of Baker map in 1000 iterations.

3. Proposed encryption and decryption algorithm

In the proposed technique of low detail image encryption, both confusion and diffusion ciphers are used. The flow charts of the proposed encryption scheme are shown in Fig. 3 and the decryption scheme are shown in Fig. 4.

3.1. Encryption algorithm

The proposed technique involves the 2D-Henon chaotic map and 2D-Baker chaotic map for diffusion and confusion operations. The encryption algorithm involves the following steps:

1. Choose high detail image $K(m, n)$ from the user secret image database.
2. Now, we have applied 2D-Henon chaotic map for the chosen secret image.
3. Employ XORing operation between the encrypted key image and low detail image.
4. The final encrypted image is obtained by using confusion operation between the image of step 3 and the sequence generated by the 2D-Baker chaotic map.

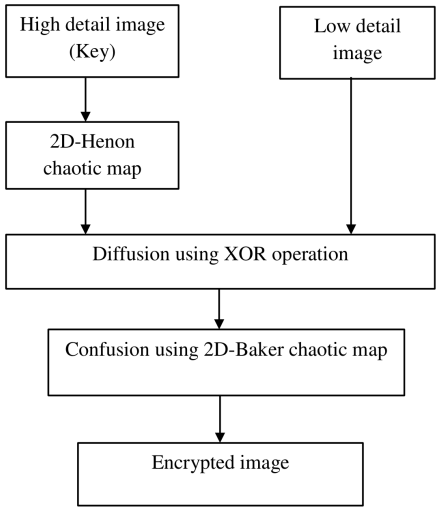


Figure 3: Block diagram of the proposed encryption scheme.

3.2. Decryption algorithm

The decryption algorithm involves the following steps:

1. Decrypt the final encrypted image using the 2D-Baker chaotic map.
2. Now, employ 2D-Henon chaotic map in the key image to obtain encrypted key image.
3. To obtain the final decrypted image, employ XORing operation between the encrypted key image and the image obtained in step 2.

4. Numerical simulation of the proposed technique

The computer based simulation of the proposed technique is performed on different low detail images. The computer system is equipped with Intel® Core™ i5-6200 processor, operating @ 2.30 GHz frequency, with 8 GB RAM and operating on Windows 10 platform using MATLAB™ R-2015a.

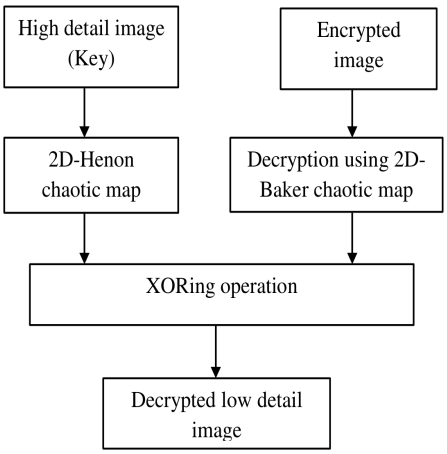
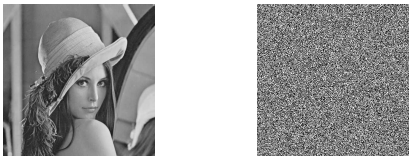


Figure 4: Block diagram of the decryption algorithm.



(a) (b)

Figure 5: (a) High detail image key, and (b) encrypted key image.

Figure 5 shows the high detail image key and encrypted key image using 2D-Henon chaotic map.

The proposed technique is applied to the low detail images of Brain, Chessboard, CS, Fingerprint, Nike, and Tux of size 512×512. The first values of 2D-Henon chaotic map are $u_0 = 0.5$ and $v_0 = 0.6$. The first values and control parameters of the 2D-Baker chaotic map are $x_0 = 0.235$, $y_0 = 0.527$, and $r_1 = 0.23$, $r_2 = 0.77$, $\alpha = 0.32$. Fig. 6(a)–(f) displays original low detail images, Fig. 6(g)–(l) displays corresponding encrypted images, and Fig. 6(m)–(r) displays corresponding decrypted images.

5. Security analysis

In this section, we have discussed key space analysis, cropping attack analysis, noise attack analysis and differential attack analysis.

5.1. Key space analysis

The proposed cryptosystem have secret parameters of 2D-Henon chaotic map and 2D-Baker chaotic map u_0, v_0 and x_0, y_0, r_1, r_2, α, respectively. If the precision is 10^{-15}, the key space will be 10^{105}, which is sufficiently large to prevent the secret key search-based attacks.

5.2. Cropping attack analysis

For the cropping attack analysis, we select the encrypted image (Fig. 6(f)). The cropped image of Fig. 6(f) are shown in Fig. 7(a)–(f). The image of Fig. 6(f) is cropped 25% from left, 50% from left, 75% from left, 50% from top, 50% from right, and 50% from middle, which are shown in Fig. 7(a)–(f), respectively. The corresponding decrypted images are shown in Fig. 7(g)–(l). Figs. 7(g)–(l) are still visual and contain mostly original visual information. It indicates that, our proposed encryption technique is potent against cropping attacks.

5.3. Noise attack analysis

The presented technique is tested against white Gaussian noise (G), Salt and pepper noise, and Speckle noise attack. The white Gaussian noise with mean 0 and standard deviation unity is applied in the encrypted image (E), which is defined by Eq. 4,

$$E_{GN} = E(1 + \gamma G), \tag{4}$$

where E_{GN} is the ciphered image with added noise G and γ is coefficient controlling the noise intensity.

Figure 8(a) shows the original Tux image considered for simulation of white Gaussian noise attack and Fig. 8(b)–(f) displayed the decrypted image of Tux with noise intensity 0.05, 0.1, 0.2, 0.3, and 0.4, respectively.

The Salt and pepper noise attack can cause pointed and unanticipated disturbances in the image pixel. The encrypted image is distorted with noise intensity 0.05, 0.1, 0.2, 0.3, and 0.4. Figure 9(a) displays the plain Tux image for simulation of Salt and pepper noise attack and Fig. 9(b)–(f) displayed the decrypted image of Tux with noise intensity 0.05, 0.1, 0.2, 0.3, and 0.4, respectively.

Figure 10(a) shows the plain Tux image considered for simulation of Speckle noise attack and Fig. 8(b)–(f) displayed the decrypted image of Tux with noise intensity 0.05, 0.1, 0.2, 0.3, and 0.4, respectively.

It is clear from Figs. 8–10 that the effect of the white Gaussian noise, Salt and pepper noise, and Speckle noise is visible to the human eyes, and hence the proposed technique is resistant to these noises.

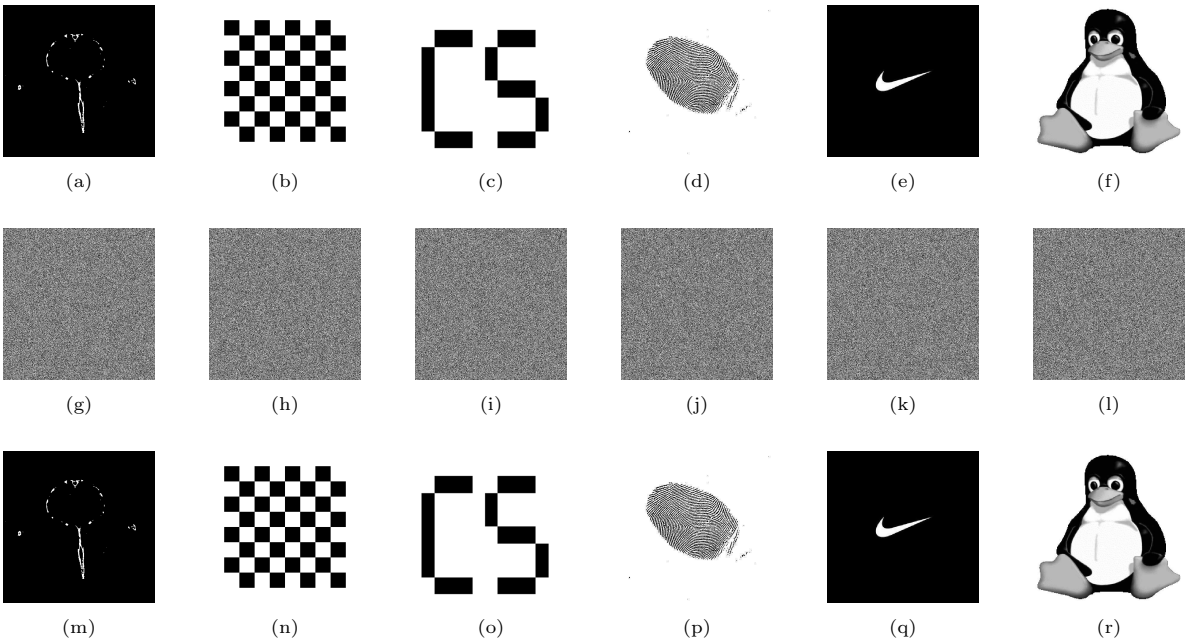


Figure 6: Experimental results of the low detail images; (a) plain image of Brain, (b) plain image of Chessboard, (c) plain image of CS, (d) plain image of Fingerprint, (e) plain image of Nike, (f) plain image of Tux, (g) ciphered image of Brain, (h) ciphered image of Chessboard, (i) ciphered image of CS, (j) ciphered image of Fingerprint, (k) ciphered image of Nike, (l) ciphered image of Tux, (m) decrypted Brain image, (n) decrypted Chessboard image, (o) decrypted CS image, (p) decrypted Fingerprint image, (q) decrypted Nike image, and (g) decrypted Tux image.

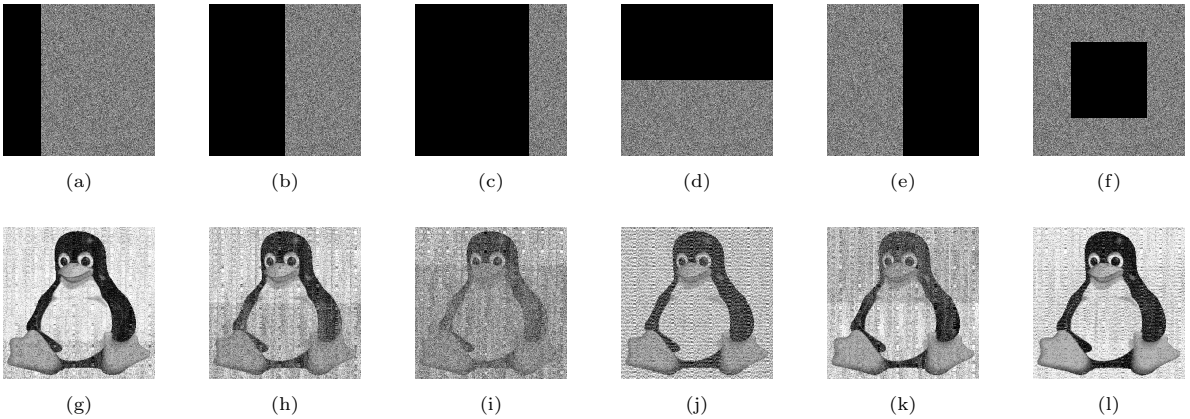
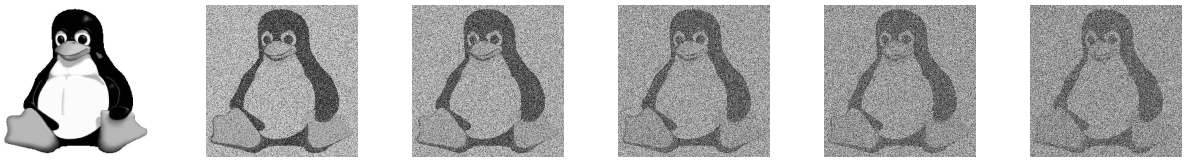


Figure 7: Experimental results of the occlusion attack in Tux image; (a) ciphered image cropped with 25% from left side, (b) ciphered image cropped with 50% from left side, (c) ciphered image cropped with 75% from left side, (d) ciphered image cropped with 50% from top, (e) ciphered image cropped with 50% from right side, (f) ciphered image cropped with 50% from middle, (g) decrypted image of image (a), (h) decrypted image of image (b), (i) decrypted image of image (c), (j) decrypted image of image (d), (k) decrypted image of image (e), and (l) decrypted image of image (f).

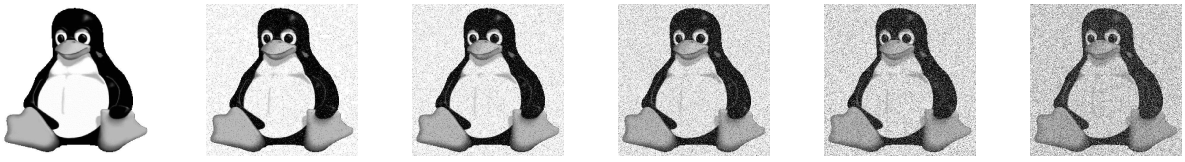
5.4. Differential attack analysis

The differential attack analysis is first analyzed by E. Biham and A. Shamir [31, 32]. In the differential attack, the adversary may change one pixel of the original image to find some meaningful relationships between the original image and the corresponding encrypted image. To understand the original image sensitivity, the number of pixels change rate (NPCR) and unified average changing intensity (UACI) [33] are given in this paper, which are



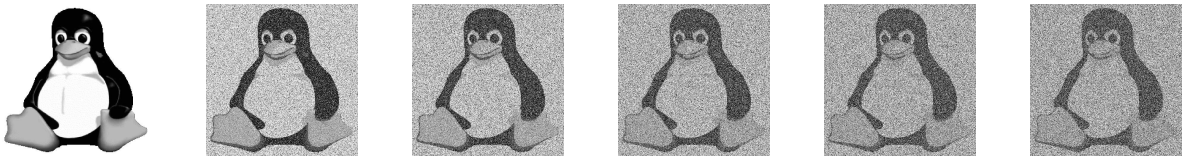
(a) (b) (c) (d) (e) (f)

Figure 8: Pictorial demonstration of white Gaussian noise attack; (a) plain image of Tux, (b) decrypted image with white Gaussian noise intensity $\gamma = 0.05$, (c) decrypted image with white Gaussian noise intensity $\gamma = 0.1$, (d) decrypted image with white Gaussian noise intensity $\gamma = 0.2$, (e) decrypted image with white Gaussian noise intensity $\gamma = 0.3$, and (f) decrypted image with white Gaussian noise intensity $\gamma = 0.4$.



(a) (b) (c) (d) (e) (f)

Figure 9: Pictorial demonstration of Salt and pepper noise attack; (a) plain image of Tux, (b) decrypted image with Salt and pepper noise intensity 0.05, (c) decrypted image with Salt and pepper noise intensity 0.1, (d) decrypted image with Salt and pepper noise intensity 0.2, (e) decrypted image with Salt and pepper noise intensity 0.3, and (f) decrypted image with Salt and pepper noise intensity 0.4.



(a) (b) (c) (d) (e) (f)

Figure 10: Pictorial demonstration of Speckle noise attack; (a) plain image of Tux, (b) decrypted image with Speckle noise intensity 0.05, (c) decrypted image with Speckle noise intensity 0.1, (d) decrypted image with Speckle noise intensity 0.2, (e) decrypted image with Speckle noise intensity 0.3, and (f) decrypted image with Speckle noise intensity 0.4.

defined by Eqs. 5 and 6, respectively,

$$\text{NPCR} = \frac{\sum_{p=1}^{P}\sum_{q=1}^{Q} D(p,q)}{P \times Q} \times 100\%, \tag{5}$$

$$\text{UACI} = \frac{1}{PQ}\left[\frac{\sum_{p=1}^{P}\sum_{q=1}^{Q} |E(p,q) - E'(p,q)|}{255}\right] \times 100\%, \tag{6}$$

where E and E' are two ciphered images corresponding to plain image with one pixel difference. $E(p,q)$ and $E'(p,q)$ denote the pixel values at the position (p,q) in the both encrypted images, respectively. P and Q are the size of the image, and $D(p,q)$ is given by Eq. 7,

$$D(p,q) = \begin{cases} 0 & \text{if} \quad E(p,q) = E'(p,q), \\ 1 & \text{if} \quad E(p,q) \neq E'(p,q). \end{cases} \tag{7}$$

For NPCR and UACI tests, we randomly choose a pixel in the plain image and change its value slightly; then, the corresponding modified encrypted image is obtained by the proposed encryption scheme. For two random images with 256×256 pixels and 24-bit true color, the expected values of NPCR and UACI [33] are 99.6094% and 33.4635%, respectively. From Table 1, the proposed technique has NPCR and UACI values very close to the standard values. So, the proposed technique is resistant to the differential attack.

6. statistical analysis

In this section, we have discussed entropy analysis, histogram analysis, error analysis, and correlation coefficient analysis.

6.1. Entropy analysis

Entropy [34] is a statistical measure of randomness of data. In case of the digital image, the en-

Standard image	Experimental values	
	NPCR(%)	UACI(%)
Brain	99.6109	0
Chessboard	99.6014	0
CS	99.6033	0
Fingerprint	99.5628	0
Nike	99.6094	0
Tux	99.4144	0

Table 1: The calculated values of NPCR and UACI performed on different standard images.

tropy $H(x)$ is calculated by Eq. 8,

$$H(x) = -\sum_{i=1}^{N} P(x_i) log_2 P(x_i), \tag{8}$$

where $P(x_i)$ denotes the probability of the symbol x_i.

The values of the entropy of the ciphered images are very close to the standard value, i.e., 8. The calculated values of the entropy of plain and ciphered images are given in Table 2.

Image	Entropy	
	Plain image	Ciphered image
Brain	0.1123	7.9976
Chessboard	1.1505	7.9976
CS	0.9319	7.9976
Fingerprint	1.4038	7.9981
Nike	0.2394	7.9976
Tux	3.4429	7.9988

Table 2: Entropy values of the plain and ciphered images.

6.2. Histogram analysis

In the case of the digital image, a histogram is a graph for the intensity of the pixels and the number of pixels. The presented technique is designed such that the scattering of pixels in the ciphered image is uniform. Figure 11(a)–(f) shows the histogram of the pain images, and Fig. 11(g)–(l) shows the histogram of the ciphered images.

6.3. Error analysis

This subsection discuss mean square error (MSE), peak signal to noise ratio (PSNR), structural similarity index metric (SSIM), and correlation coefficients of the plain and ciphered images.

6.3.1. MSE, PSNR, and SSIM analysis

Equations 9 and 10 defined the expression for calculating MSE and PSNR between the plain and ciphered images.

$$\mathrm{MSE}(f, \hat{f}) = \frac{1}{kl} \sum_{u=1}^{k} \sum_{v=1}^{l} [f(u,v) - \hat{f}(u,v)]^2 \tag{9}$$

$$\mathrm{PSNR}(f, \hat{f}) = 10 \log_{10} \frac{(255)^2}{\mathrm{MSE}(f, \hat{f})} \quad \mathrm{dB} \tag{10}$$

where $f(u,v)$ is the plain image, $\hat{f}(u,v)$ is the ciphered image, k, and l are the numbers of pixels in the image.

Higher the values of MSE and lower the values of PSNR shows that the encryption is stronger, because it shows the ciphered image contains negligible amounts of original information.

Also, The PSNR between the plain and the decrypted images can be used to evaluate the robustness of the proposed encryption scheme against noise in the decryption process. In this case, The high values of the PSNR imply the plain and decrypted images are alike.

The similarity between the two images is analyzed by SSIM. The low values of SSIM indicate that both the images are dissimilar. The SSIM index between f and $\hat{f}$ is calculated by Eq. 11,

$$\mathrm{SSIM}(I, E) = \frac{(2\mu_I \mu_E + J_1)(2\sigma_{IE} + J_2)}{(\mu_I^2 + \mu_E^2 + J_1)(\sigma_I^2 + \sigma_E^2 + J_2)}, \tag{11}$$

where μ_I and μ_E are mean, σ_I and σ_E are the standard deviation of, σ_{IE} is the covariance between f and $\hat{f}$, $J_1 = (k_1 L)^2$, $J_2 = (k_2 L)^2$, $k_1 = 0.01$, $k_2 = 0.03$, and $L = 2^{\text{number of bits per pixel}} - 1$.

Table 3 shows MSE, PSNR, and SSIM values between the plain and ciphered images.

Image	MSE	PSNR	SSIM
Brain	21696	4.8010	0.0002
Chessboard	21354	4.8700	0.0068
CS	21447	4.8511	0.0069
Fingerprint	21433	4.8540	0.0066
Nike	21676	4.8050	0.0001
Tux	18852	5.4112	0.0077

Table 3: MSE, PSNR, and SSIM values between Fig. 6(a)–(f) and Fig. 6(g)–(l), respectively.

Table 4 shows PSNR values between the plain and decrypted images at different signal to noise ratio (SNR).

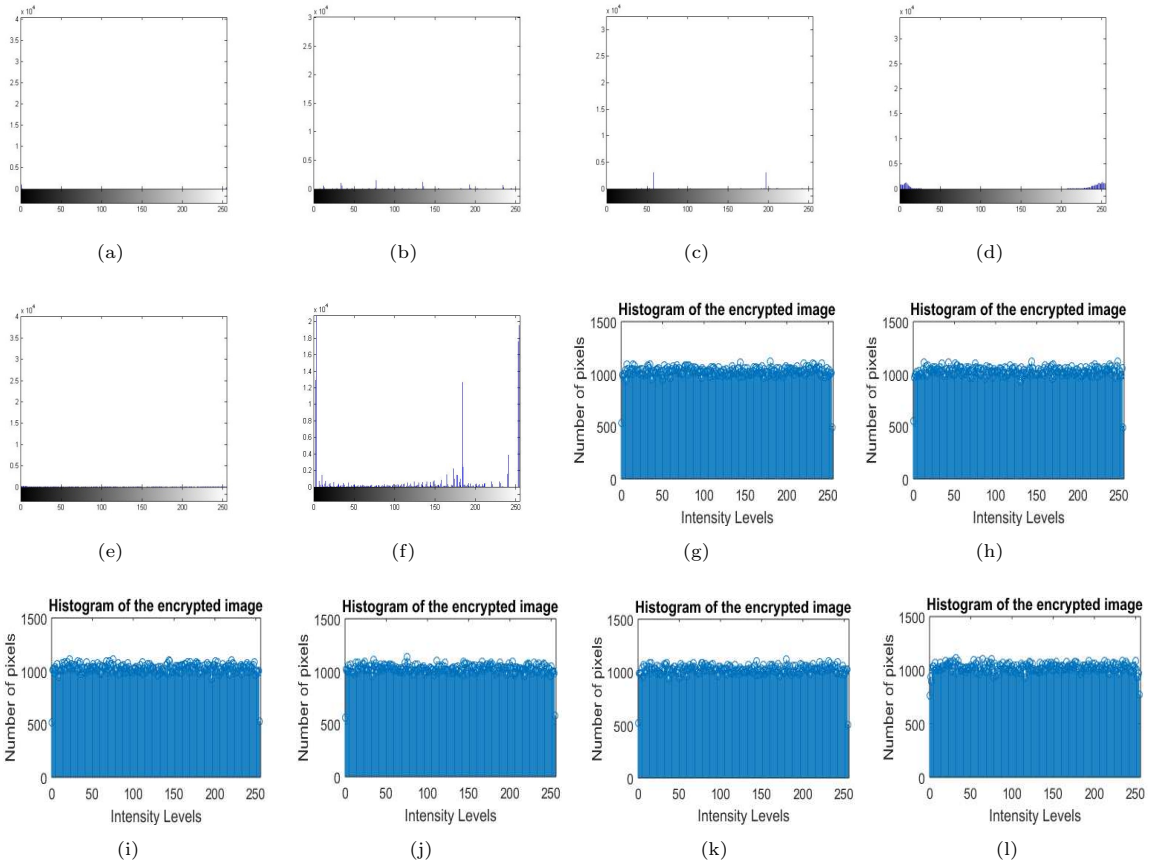


Figure 11: Experimental results of the histogram; (a) histogram of the plain image of Brain, (b) histogram of the plain image of Chessboard, (c) histogram of the plain image of CS, (d) histogram of the plain image of Fingerprint, (e) histogram of the plain image of Nike, (f) histogram of the plain image of Tux, (g) histogram of the ciphered image of Brain, (h) histogram of the ciphered image of Chessboard, (i) histogram of the ciphered image of CS, (j) histogram of the ciphered image of Fingerprint, (k) histogram of the ciphered image of Nike, and (l) histogram of the ciphered image of Tux.

Image	PSNR				
	SNR= 0 dB	10 dB	20 dB	30 dB	40 dB
Brain	13.1	17.18	21.78	26.72	39.7
Chessboard	14.56	16.67	20.23	24.68	29.74
CS	16.13	18.32	22	26.7	31.68
Fingerprint	19.61	22	25.45	29.68	35.03
Nike	12.61	16.44	21	26.03	36.11
Tux	15.05	17.32	20.91	25	29.5

Table 4: PSNR values for the decrypted images in the existing noise.

6.4. Correlation analysis

The robustness of the presented technique with respect to the pixel intensity distribution of adjacent pixels in horizontal, vertical, and diagonal directions by calculating the correlation coefficient C_{xy} of two adjacent pixels x and y in an image using Eq. 12,

$$C_{xy} = \frac{\sum_{i=1}^{u}\sum_{j=1}^{v}(x_{i,j}-\overline{x})(y_{i,j}-\overline{y})}{\sqrt{[\sum_{i=1}^{u}\sum_{j=1}^{v}(x_{i,j}-\overline{x})]^2[\sum_{i=1}^{u}\sum_{j=1}^{v}(y_{i,j}-\overline{y})]^2}}, \tag{12}$$

where $x_{i,j}$ and $y_{i,j}$ represent the pixel in the i^{th}-row and j^{th}-column, $\overline{x}$ and $\overline{y}$ are mean of the adjacent pixels.

For a plain image, it has a value close to 1 or −1 as adjacent pixels are highly correlated. But, in a ciphered image, the value of C_{xy} is near to 0. We calculate the C_{xy} in horizontal, vertical and diagonal directions for the Brain, Chessboard, CS, Fingerprint, Nike, and Tux images. The values of plain and ciphered images are shown in Tables 5 and 6, respectively. For each direction (horizontal, vertical or diagonal) of the ciphered images, the C_{xy} is near to 0. Thus, there is a very negligible correlation of adjacent pixels in the images ciphered by the presented technique even the adjacent pixels in the plain images are highly correlated.

Fig. 12 shows the graph of the pixel intensity distribution of adjacent pixels in the original and encrypted images along horizontal, vertical, and diagonal directions.

Plain image	Direction		
	Horizontal	Vertical	Diagonal
Brain	0.7504	0.8392	0.7340
Chessboard	0.9816	0.9816	0.9635
CS	0.9929	0.9931	0.9860
Fingerprint	0.7390	0.6524	0.4846
Nike	0.9855	0.9640	0.9431
Tux	0.9833	0.9856	0.9729

Table 5: Correlation coefficient values of plain low detail image of Brain, Chessboard, CS, Fingerprint, Nike, and Tux.

Ciphered image	Direction		
	Horizontal	Vertical	Diagonal
Brain	0.0001	−0.0012	−0.0030
Chessboard	0.0010	0.0007	0.0002
CS	−0.0009	−0.0029	−0.0036
Fingerprint	−0.0008	−0.0007	−0.0032
Nike	−0.0005	−0.0011	−0.0033
Tux	−0.0002	−0.0015	−0.0018

Table 6: Correlation coefficient values of ciphered image of Brain, Chessboard, CS, Fingerprint, Nike, and Tux.

7. Conclusion

In this paper, we have presented a new technique for low detail images based on diffusion and confusion using Henon chaotic map and Baker chaotic map. The proposed technique is a confusion-diffusion-based encryption technique for the security of low detail images using high detail image as secret key.

Funding: No funding.

Author's contribution: All authors are contributed in this work.

Code availability: We are used our own data and coding.

Declarations

Conflict of interest : No conflict of interest.

Humans and animals rights: Humans and animals are not involved in this work.

References

[1] G. Gu, J. Ling. A fast image encryption method by using chaotic 3D cat maps. Optik. 125(17):2014;4700–4705.

[2] G. Ye, K.W. Wong. An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dynamics. 69:2012;2079–2087.

[3] L. Gong, C. Deng, S. Pan, N. Zhou. Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform. Opt Laser Technol. 103:2018;48–58.

[4] A.B. Joshi, D. Kumar, D.C. Mishra, V. Guleria. Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map. J Mod Opt. 67(10):2020;933–949.

[5] A.B. Joshi, D. Kumar, A. Gaffar, D.C. Mishra. Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform. Opt Lasers Eng. 133:2020;106139–106151.

[6] O.S. Faragallah, A. Afifi, I.F. Elashry, E.A. Naeem, H.M. El-Hoseny, H.S. El-sayed, A.M. Abbas. Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform. Opt Quant Electron. 53(6):2021;1–26. https://doi.org/10.1007/s11082-021-02864-5.

[7] O.S. Faragallah, M.A. AlZain, H.S. El-Sayed, J.F. Al-Amri, W. El-Shafai, A. Afifi, E.A. Naeem, B. Soh. Secure color image cryptosystem based on chaotic logistic in the FrFT domain. Multimed Tools Appl. 79:2020;2495–2519. https://doi.org/10.1007/s11042-019-08190-z.

[8] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, E.A. Naeem, M.A. Alzain, J.F. Al-Amri, B. Soh, F.E. Abd El-Samie. Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications. IEEE Access. 8:2020;42491–42503. 10.1109/ACCESS.2020.2974226.

[9] D. Kumar, A.B. Joshi, S. Singh, V.N. Mishra, H.G. Rosales, L. Zhou, A. Dhaka, A. Nandal, H. Malik, S. Singh. 6D-Chaotic System and 2D Fractional Discrete Cosine Transform Based Encryption of Biometric Templates. IEEE Access. 9:2021;103056–103074. 10.1109/ACCESS.2021.3097881.

[10] A.B. Joshi, D. Kumar, D.C. Mishra. Security of digital images based on 3D Arnold Cat map and elliptic curve. Int J Image Graphics. 21(1):2021;2150006–2150026. https://doi.org/10.1142/S0219467821500066.

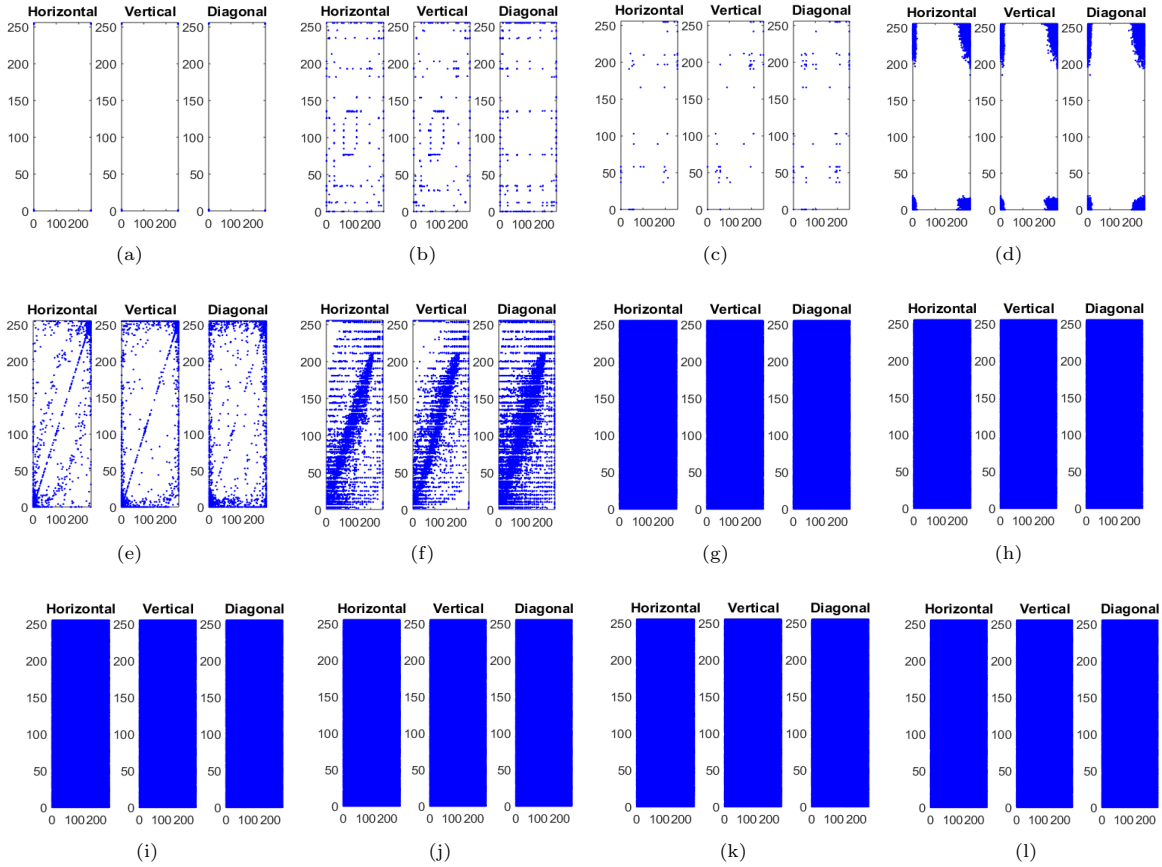


Figure 12: Correlation coefficient along horizontal, vertical, and diagonal direction of; (a) original Brain image, (b) original Chessboard image, (c) original CS image, (d) original Fingerprint image, (e) original Nike image, (f) original Tux image, (g) encrypted Brain image, (h) encrypted Chessboard image, (i) encrypted CS image, (j) encrypted Fingerprint image, (k) encrypted Nike image, and (l) encrypted Tux image.

[11] E. Naeem, M.M.A. Elnaby, N.F. Soliman, A.M. Abbas, O.S. Faragallah, N.A.E. Semary, M.M. Hadhoud, S.A. Alshibeili, F.E.A. El-Samie. Efficient Implementation of Chaotic Image Encryption in Transform Domains. Journal of Systems and Software. 97:2014;118–127. https://doi.org/10.1016/j.jss.2014.07.026.

[12] C. Li. Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Process. 118:2016;203–210. https://doi.org/10.1016/j.sigpro.2015.07.008.

[13] S. Anwar, S. Meghana. A pixel permutation based image encryption technique using chaotic map. Multimed Tools Appl. 78:2019;27569–27590. https://doi.org/10.1007/s11042-019-07852-2.

[14] C. Li, D. Lin, J. Lu. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE Multi Media. 24(3):2017;64–71. 10.1109/MMUL.2017.3051512.

[15] C. Li, K.T. Lo. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. 91(4):2011;949–954. https://doi.org/10.1016/j.sigpro.2010.09.014.

[16] C. Zhu. A novel image encryption scheme based on improved hyperchaotic sequences. Opt Commun. 285(1):2012;29–37. https://doi.org/10.1016/j.optcom.2011.08.079.

[17] F. Ozkaynak, A.B. Ozer, S. Yavuz. Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences. Opt Commun. 285(24):2012;4946–4948. https://doi.org/10.1016/j.optcom.2012.07.106.

[18] C. Li, Y. Liu, T. Xie, M.Z.Q. Chen. Breaking a novel image encryption scheme based on improved hyperchaotic sequences. Nonlinear Dyn. 73:2013;2083–2089. https://doi.org/10.1007/s11071-013-0924-6.

[19] G. Ye, J. Zhou. A block chaotic image encryption scheme based on self-adaptive modelling. Applied Soft Computing. 22:2014;351–357. https://doi.org/10.1016/j.asoc.2014.05.025.

[20] W.S. Yap, R.C.W. Phan. Commentary on "A block chaotic image encryption scheme based on self-adaptive modelling" [Applied Soft Computing 22 (2014) 351–357]. Applied Soft Computing. 52:2017;501–504. https://doi.org/10.1016/j.asoc.2016.10.018.

[21] J. Fridrich. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. Int J Bifurcation Chaos. 8(6):1998;1259–1284. https://doi.org/10.1142/S021812749800098X.

[22] Y. Li, C. Wang, H. Chen. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Lasers Eng. 90:2017;238–246. https://doi.org/10.1016/j.optlaseng.2016.10.020.

[23] S.F. Raza, V. Satpute. A novel bit permutation-based image encryption algorithm. Nonlinear Dyn. 95:2019;859–873. https://doi.org/10.1007/s11071-018-4600-8.

[24] W. Liu, K. Sun, C. Zhu. A fast image encryption algorithm based on chaotic map. Opt Lasers Eng. 84:2016;26–36. https://doi.org/10.1016/j.optlaseng.2016.03.019.

[25] R. Hamza, F. Titouna. A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective. 25(4–6):2016;162–179. https://doi.org/10.1080/19393555.2016.1212954.

[26] P. Ping, F. Xu, Y. Mao, Z. Wang. Designing permutation–substitution image encryption networks with Henon map. Neurocomputing. 283:2018;53–63. https://doi.org/10.1016/j.neucom.2017.12.048.

[27] K. Mishra, R. Saharan. A fast image encryption technique using Henon chaotic map. Progress in advanced computing and intelligent engineering, Springer, Singapore. 2019, pp. 329–339. https://doi.org/10.1007/978-981-13-1708-8_30.

[28] M. Henon. A two-dimensional mapping with a strange attractor. The theory of chaotic attractors. Springer, New York. 1976, pp. 94–102. https://doi.org/10.1007/978-0-387-21830-4_8.

[29] L. Liu, S. Miao. An image encryption algorithm based on Baker map with varying parameter. Multimedia Tools and Applications. 76:2017;16511–16527.

[30] J.W. Yoon, H. Kim. An image encryption scheme with a pseudorandom permutation based on chaotic maps. Commun Non Sci Num Simulat. 15(12):2010;3998–4006.

[31] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. J Cryptol. 4(1):1991;3–72.

[32] E. Biham, A. Shamir. Differential cryptanalysis of the Full 16-Round DES. Annual Int Cryptology Conf., Springer, Heidelberg. 1992, pp. 487–496.

[33] Y. Wu, J.P. Noonan, S. Agaian. NPCR and UACI randomness tests for image encryption. J Selected Areas Telecommun. 1(2):2011;31–38.

[34] C.E. Shannon. A mathematical theory of communication. Bell System Tech J. 27(3):1948;379–423.