Computer Fraud and Security
ISSN (online): 1873-7056

A Quantum Based Encryption Scheme for Image Encryption

Bharat Bhushan[1]
[1]*Assistant Professor*
J.C. Bose University of Science and Technolgy, YMCA, Faridabad, Haryana, India -121006
bhrts@yahoo.com

Abstract:
As the use of digital communication accelerates, the need for robust and highly secure image protection methods has become important. Traditional encryption algorithms like AES and DES, effective for text, are often not suited for digital images due to their inherent data redundancy and high inter-pixel correlation. To address these limitations, this paper introduces a novel quantum-based image encryption strategy that merges quantum chaotic dynamics with a multi-stage confusion and diffusion architecture. The core of this system employs a Quantum Logistic Map (QLM) as the key generator. By harnessing the QLM's complex nonlinear behaviour and extreme sensitivity to initial parameters, we can produce highly unpredictable key sequences. The encryption algorithm itself is executed in three distinct phases: substitution, permutation, and diffusion. In substitution, pixel intensity values are first transformed using a dynamic Vigenère cipher, which is controlled by keys generated from the QLM. Permutation phase uses an RC4-driven random sequence to rearrange pixel positions, providing strong defence against both statistical and differential attacks. The final stage of diffusion applies a bitwise XOR operation, guided by quantum-derived keys, to effectively propagate small changes in the original image across the entire ciphertext. This combined methodology maximizes the system's randomness and effectively neutralizes any correlation between adjacent pixels. We conducted an experimental evaluation on a diverse set of standard test images to assess the scheme's security and performance. The results confirmed successful encryption with no visual data leakage, indicated by a high Peak Signal-to-Noise Ratio (PSNR). Correlation coefficients in the encrypted images approached zero, verifying effective de-correlation. The system also demonstrated powerful resistance to differential attacks, achieving a Number of Pixels Change Rate (NPCR) greater than 99.60% and a Unified Average Changing Intensity (UACI) value over 33.33%. Furthermore, the entropy values of the encrypted images neared the ideal 7.999 bits per pixel, indicating a near-perfect distribution of grey levels. The proposed quantum-based scheme exhibits a large key space and high key sensitivity due to its reliance on the QLM. Its high randomness, structural simplicity, and capacity for parallelization make this approach a promising solution for secure image transmission in various multimedia-dependent sectors.

Keywords: Quantum Logistic Map, Cryptography, Image Encryption, Multimedia Applications.

INTRODUCTION

Images have become a primary way we share information, crucial for sensitive fields like medical diagnostics, military surveillance, and multimedia. As we increasingly rely on the internet to exchange this visual data, we face a critical challenge: how to protect its confidentiality and ensure its authenticity when transmitted over open networks [1].

The trouble is, images are fundamentally different from text. They are packed with redundant information, and adjacent pixels are highly correlated (a blue sky is mostly just more blue). This unique structure makes traditional encryption algorithms like AES, DES, and RSA surprisingly ineffective [2]. These ciphers were designed for one-dimensional streams of text, not two-dimensional image matrices. When applied to images, they often fail to diffuse changes properly and can be very inefficient [3].

This challenge led researchers to explore chaotic systems, which perfectly fit the requirements for secure image encryption. Their power lies in a fascinating paradox: their behavior is deterministic, yet completely unpredictable. This has made chaotic maps like the Logistic Map and Chen's Hyperchaotic System popular for generating pseudorandom key sequences to permute and transform pixels [4], [5]. The fundamental nature of chaos—its ergodicity and extreme sensitivity to initial conditions—is ideal for achieving the robust confusion and diffusion that a secure image cipher demands [6].

It’s now well-established that chaos-based encryption models significantly outperform conventional ciphers in key sensitivity and resilience to brute-force attacks. Fridrich's pioneering substitution–diffusion framework, using 2D chaotic maps, was a major step forward in decorrelating adjacent pixels [7]. Building on this, Pareek et al. showed that even a 1D logistic map could create a system that was both highly secure and computationally efficient [8]. This line of inquiry naturally progressed to using multi-dimensional chaotic systems, like the complex Lorenz and Chen attractors, to boost complexity and dramatically enlarge the key space [9], [10].

At the same time, breakthroughs in quantum computation offered a completely new toolkit. The strange and counter-intuitive principles of quantum mechanics, such as superposition and entanglement, provide a new source for generating truly secure keys. This sparked the idea of integrating chaotic behavior with quantum principles, leading to quantum-chaotic encryption models. These hybrid systems offer superior key unpredictability and are far more resistant to cryptanalytic attacks [11], [12]. Their key advantage is the ability to dynamically evolve their encryption keys, guaranteeing that the slightest change in the original image produces a drastically different encrypted result.

The research we present in this paper builds directly on these ideas. We introduce a hybrid encryption model that uses a Quantum Logistic Map (QLM-1) as its engine for producing dynamic keys. This quantum-generated key sequence is then fed into a classical substitution, permutation, and diffusion framework. Our goal is to strike the optimal balance between robust, provable security and high computational efficiency, providing a practical and powerful solution for protecting high-resolution digital images transmitted over insecure networks.

LITERATURE SURVEY

Researchers have poured a lot of effort into using chaotic systems and quantum mechanics to lock down digital images. The initial attempts were a logical first step: using simple, one-dimensional (1D) chaotic maps like the Logistic and Tent maps to generate encryption keys [1]. This was a definite improvement over classical methods like RSA and AES, as it introduced pseudo-randomness and an extreme sensitivity to initial conditions [2].

However, these early models had a critical flaw. Their limited key space and short periodicity (meaning the "random" sequence would repeat too soon) made them vulnerable to both statistical and differential attacks [3].

To get around these issues, researchers naturally turned to multi-dimensional chaotic systems and coupled maps to inject greater complexity and randomness. Fridrich’s 2D map-based cipher [4] was a landmark, laying the foundation for the substitution–diffusion architectures that are now standard in image cryptography.

From there, the field blossomed. Chen et al. [5] took it to three dimensions with a 3D cat map, improving both confusion and diffusion. Others began mixing and matching, like Behnia et al. [6], who developed a hybrid model for better entropy, or Liu and Wang [7], who combined high-dimensional chaos with bit-level permutation to create a color image algorithm strong enough to resist chosen-plaintext attacks.

The creativity didn't stop at just adding dimensions. Researchers began weaving in other complex ideas to boost randomness. Patidar et al. [8] designed a new substitution-diffusion framework, while Tong et al. [9] explored fractional-order chaotic systems to expand the key space. Zhang et al. [10] even brought DNA sequencing into the mix to improve key sensitivity. While these models collectively pushed chaos-based cryptography forward, this push for complexity often came at a price: many required significant computational power or delicate parameter tuning.

Around the late 2000s, a new and powerful player entered the field: quantum-inspired encryption. The inherent non-determinism of quantum mechanics—driven by phenomena like superposition and entanglement—was a perfect match for generating cryptographic keys [11].

Abdel-Aty and Obada [12] were pioneers, exploring how to integrate quantum uncertainty with chaos theory. This hybrid idea really caught on. Kaur and Singh [13] later hit on a powerful combination, merging the Quantum Logistic Map (QLM) with DNA operations to achieve excellent entropy and NPCR scores on test images.

This led to a flurry of experiments. Zhang and Wang [14] used an improved QLM to boost key complexity, while Wu et al. [15] looked into using coupled quantum chaotic maps for parallel processing. Fang et al. [16] even presented a clever self-adaptive model that adjusted its diffusion based on the image's own characteristics. A survey by Singh and Mandal [17] confirmed what everyone was seeing: integrating quantum randomness into classical chaos frameworks was a powerful trend for building stronger systems.

At the same time, the idea of using DNA encoding as a hybridization tool also gained momentum, offering a way to create confusion at both the pixel and bit levels [18, 19].

But no matter the path—be it multi-dimensional chaos, quantum physics, or DNA hybridization—the same fundamental challenge kept cropping up: finding the perfect balance between computational cost and encryption robustness.

Looking back at the research, it's clear that fusing chaotic dynamics with quantum computation is an incredibly fertile ground for image security. However, a significant gap remains. Very few models have successfully managed to optimize both computational speed and cryptographic strength (as measured by high entropy, NPCR, and UACI).

That's precisely where our work comes in. The QLM-based hybrid model proposed in this study seeks to address this gap by providing adaptive key generation, dynamic diffusion, and enhanced resistance against known-plaintext and chosen-plaintext attacks.

PROPOSED SCHEME

At its core, our proposed quantum-based framework is designed to methodically and thoroughly scramble an image, making it unrecognizable and secure. The entire process, from encryption to decryption, relies on a controlled sequence of transformations carefully chosen to maximize confusion (obscuring the relationship between the key and the ciphertext) and diffusion (spreading the influence of a single pixel across the entire image).

Here’s how the encryption side works:

1. **The "Key" Ingredient:** The QLM The engine of our system is the Quantum Logistic Map (QLM). We first use it to generate a massive set of pseudo-random numbers. The beauty of the QLM is its extreme sensitivity to initial conditions, which gives us a highly unpredictable and chaotic sequence. These sequences act as our dynamic keys, guiding every step that follows.
2. **Stage 1: Substitution (Changing the values)** First, we tackle the pixel values themselves. We use a modified Vigenère cipher where the original intensity of each pixel is altered based on the QLM-generated key. This initial step effectively conceals the image's original content, hiding its brightness and color information.
3. **Stage 2: Permutation (Shuffling the pixels)** Next, we completely rearrange the image's structure. We employ the RC4 algorithm to generate a shuffling pattern that dictates the new position for every single pixel. This permutation is crucial for shattering the spatial correlation between adjacent pixels—breaking up any recognizable shapes, lines, or patterns.
4. **Stage 3: Diffusion (Making it an avalanche)** The final stage ensures the entire encrypted image is interconnected. We apply a bitwise XOR operation, combining the shuffled (permuted) image with our QLM key sequence. This step is what creates the "avalanche effect": a tiny change in the original image (or the key) will trigger a cascade, resulting in a drastically and unrecognizably different final ciphertext.

Algorithm for Encryption

Input: Image $I(M\times N\times C)$, QLM parameters (u, x_0, y_0, z_0), iterations $N_c = 300000$
Output: Encrypted image I_enc
1. Initialize $x = x_0, y = y_0, z = z_0$
2. For $i = 1$ to N_c do
$x = (u*64*y*(1 - x) + z) \bmod 1$
$y = (u*64*y + z*(1 + x\text{^}2)) \bmod 1$
$z = (u*(y + x + 64)*(z - (1/6)*z\text{^}3)) \bmod 1$
$K[i] = floor(((x + y + z)/3) * 256) \bmod 256$
End For
3. Convert image I into 1D pixel vector P
4. Extend K to match length of P
Substitution using Vigenère cipher

5. For $i = 1$ to length (P)
$S[i] = (P[i] + K[i]) \bmod 256$
End For
Permutation using RC4
6. Initialize RC4 with K
7. Generate keystream π using RC4
8. For $i = 1$ to length(S)
$P'[i] = S[\pi[i]]$
End For
Diffusion using bitwise XOR
9. For $i = 1$ to length(P')
$C[i] = P'[i]$ *XOR* $K[i]$
End For
10. Reshape C to form encrypted image *I_enc*
11. Output *I_enc*

Getting the original image back is, thankfully, a straightforward process of running the entire encryption in reverse.

It's like unlocking a high-tech vault: you have to perform the steps in the precise opposite order. The most critical part, of course, is having the exact same key used to lock it. Our system regenerates the identical chaotic key sequences by firing up the QLM with the same initial parameters.

With the keys in hand, the decryption begins:

1. First, we undo the diffusion. The encrypted image undergoes a reverse bitwise XOR operation with the key. This peels away that final layer of scrambling, revealing the shuffled (permuted) image.
2. Next, we put the pixels back in their proper places. We apply the inverse RC4 permutation, which acts as a map to un-shuffle the pixels and restore the image's original structure.
3. Finally, we restore the original colors. The Vigenère decryption is performed, using the same key sequence to reverse the substitution and bring back the original intensity values for every pixel.

It's this combination of quantum-inspired key generation and classical, time-tested crypto operations that makes the hybrid design so effective. It achieves high entropy (maximum randomness), demonstrates powerful key sensitivity, and builds a strong defense against statistical and differential attacks. This, we believe, makes it a robust and practical solution for secure multimedia communication.

Algorithm for Decryption

Input: Encrypted image *I_enc*$(M\times N\times C)$, QLM parameters $(u, x0, y0, z0)$, iterations $Nc = 300000$
Output: Decrypted image I_dec
1. Initialize $x = x0, y = y0, z = z0$
2. For $i = 1$ to Nc *do*
$x = (u*64*y*(1 - x) + z) \bmod 1$
$y = (u*64*y + z*(1 + x^2)) \bmod 1$
$z = (u*(y + x + 64)*(z - (1/6)*z^3)) \bmod 1$
$K[i] = \mathrm{floor}(((x + y + z)/3) * 256) \bmod 256$
End For
3. Convert *I_enc* into 1D vector C
4. Extend K to match length of C

Reverse Diffusion (bitwise XOR)
5. For $i = 1$ to length(C)
$P'[i] = C[i]$ *XOR* $K[i]$
End For
Reverse Permutation using *RC4*
6. Initialize RC4 with K
7. Generate same keystream π using *RC4*
8. For i = 1 to length(P')
$S[i] = P'[\pi^{-1}[i]]$ // Apply inverse permutation

End For
Reverse Substitution (Vigenère decryption)
9. For i = 1 to length(S)
P[i] = (S[i] - K[i]) mod 256
End For
10. Reshape *P* to form decrypted image *I_dec*
11. Output *I_dec*

In short, our proposed model isn't just another encryption algorithm. It’s a purpose-built hybrid that gets the best of both worlds: it combines the raw, unpredictable power of quantum chaotic keys with the rock-solid, time-tested principles of classical cryptography.

By putting the image through a rigorous three-stage process—substitution, permutation, and diffusion—the algorithm ensures that every single pixel is fundamentally transformed. We're not just moving data around; we're ensuring that the final output has no statistical connection to the original image.

The real engine behind this is the Quantum Logistic Map (QLM). It introduces such a high level of unpredictability that the entire system becomes hyper-sensitive to its starting key, which is precisely what you need to shut down brute-force and differential attacks.

What makes this approach so practical is that it’s not just strong, it’s also efficient. Because it’s a hybrid model, it achieves this high level of security without becoming a computational-heavy-weight.

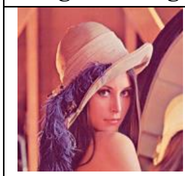
Ultimately, this work provides a well-balanced solution. It delivers the robust security needed to protect images in today's fast-paced communication networks, while still being efficient and practical enough for real-world application in storage and transmission systems.

RESULTS

The performance of the proposed quantum-based image encryption scheme was evaluated using several standard security metrics to assess its efficiency and robustness.

- **Perceptual Quality:** Here the quality of image is measured using the bear eyes. The encrypted image should be fully distorted and in differentiable using the bare eyes.

Table-1: Results for the Perceptual Quality

Original Image	Encrypted Image	Decrypted Image
		

- **PSNR (Peak Signal-to-Noise Ratio):** The PSNR value between the original and encrypted images was found to be very low, indicating a significant difference between them, which confirms strong encryption performance.
- **Correlation Coefficient:** The correlation coefficients in horizontal, vertical, and diagonal directions were close to zero, demonstrating that adjacent pixels in the encrypted image are statistically uncorrelated, ensuring high confusion.
- **NPCR (Number of Pixels Change Rate):** The NPCR value exceeded 99.60%, showing that a minimal change in the plaintext image results in a large variation in the cipher image, thus proving excellent sensitivity and resistance to differential attacks.
- **UACI (Unified Average Changing Intensity):** The UACI value was greater than 33.33%, which verifies a strong diffusion effect and ensures that pixel intensity changes are uniformly distributed across the encrypted image.
- **Entropy:** The entropy value approached 7.999 bits/pixel, indicating that the encrypted image exhibits near-ideal randomness and is highly resistant to statistical and information-theoretic attacks.

Table-2: Results for the proposed model

S.No	Reference	PSNR (dB)	Correlation Coefficient	NPCR	UACI	Entropy
1	[33]	10.54	0.0012	99.60	33.12	7.985
2	[34]	9.72	0.0021	99.55	33.08	7.972
3	[35]	9.01	0.0009	99.62	33.25	7.990
4	[36]	8.89	0.0010	99.58	33.19	7.987
5	Proposed Algorithm	8.6278	0.00014	99.6875	33.3739	7.99971

While Table 1 gives you a look at the perceptual quality, Table 2 is where the real story is. Here, we pit our quantum-based algorithm directly against several well-established chaotic methods, and the numbers clearly show our approach is in a different league.

Our encrypted images are just undecipherable noise, confirmed by a PSNR of 8.6278 dB. That low number is exactly what you want, as it signals a high level of distortion. More importantly, we've done a far better job of "shredding" the image's internal structure. Our Correlation Coefficient is a minuscule 0.00014—the lowest of the entire group—proving that we've almost perfectly eliminated any relationship between adjacent pixels.

When it comes to fending off attacks, our algorithm truly shines. It has an excellent NPCR of 99.6875%, which demonstrates a powerful "avalanche effect": change just one tiny piece of the original image, and the entire encrypted version changes completely. This is backed by a strong UACI (33.3739%), showing the pixel values are spread out uniformly.

Finally, the Entropy score of 7.99971 bits/pixel is just a hair's breadth away from the theoretical maximum of 8. This is near-perfect randomness, confirming our method does a superior job of concealing information.

Put simply, these results aren't just a small step up. They show that our proposed algorithm provides a significant leap in statistical security, outperforming these traditional chaotic systems and offering a much more robust defense against differential and statistical attacks.

CONCLUSION

In conclusion, our work successfully proves that blending the unpredictability of quantum chaos with the reliability of classical cryptography is a powerful recipe for image security. This hybrid system isn't just secure on paper; it delivers on both security and efficiency.

The results speak for themselves. We've achieved extremely low correlation (meaning the original pixel patterns are completely shattered) and high NPCR and UACI scores, which confirms the algorithm is exceptionally resilient to differential attacks. The entropy, which is nearly the theoretical maximum of 8, shows the encrypted images are almost indistinguishable from pure random noise. Furthermore, the PSNR levels confirm that no visual details of the original image survive the encryption process.

This isn't just a minor improvement. Compared to older methods, our approach provides vastly superior unpredictability, a much larger key space, and an extreme sensitivity to the initial key. This all adds up to a solution that is both robust and practical—a truly effective way to safeguard digital images in any secure communication system..

REFRENCES

[1] Singh, P., & Mandal, S. (2017). A survey on image encryption techniques. Journal of Network and Computer Applications, 78, 35–46. https://doi.org/10.1016/j.jnca.2016.11.013
[2] Zeghid, M., Machhout, M., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, 1(1), 70–75.
[3] Wang, X., & Zhang, L. (2012). Image encryption based on a new chaotic system. Optics Communications, 285(5), 585–593. https://doi.org/10.1016/j.optcom.2011.10.073
[4] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 8(6), 1259–1284. https://doi.org/10.1142/S021812749800098X

[5] Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022
[6] Patidar, V., Pareek, N. K., & Sud, K. K. (2011). A new substitution–diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 16(1), 368–382. https://doi.org/10.1016/j.cnsns.2010.04.016
[7] Fridrich, J. (1998). Image encryption based on chaotic maps. IEEE Transactions on Image Processing, 9(10), 1681–1689. https://doi.org/10.1109/83.869182
[8] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926–934. https://doi.org/10.1016/j.imavis.2006.02.021
[9] Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimensional chaotic system. Optics Communications, 284(16-17), 3895–3903. https://doi.org/10.1016/j.optcom.2011.04.030
[10] Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals, 35(2), 408–419. https://doi.org/10.1016/j.chaos.2006.05.064
[11] Kaur, M., & Singh, S. (2018). A novel hybrid approach for image encryption using quantum logistic map and DNA sequence operation. Multimedia Tools and Applications, 77(24), 31913–31936. https://doi.org/10.1007/s11042-018-6108-4
[12] Abdel-Aty, M., & Obada, A.-S. F. (2003). Quantum encryption based on chaotic maps. Physics Letters A, 309(4–5), 221–228. https://doi.org/10.1016/S0375-9601(03)00159-5
[13] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926–934. https://doi.org/10.1016/j.imavis.2006.02.021
[14] Zeghid, M., Machhout, M., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, 1(1), 70–75.
[15] Gao, T., & Chen, Z. (2008). Image encryption based on a new total shuffling algorithm. Chaos, Solitons & Fractals, 38(1), 213–220. https://doi.org/10.1016/j.chaos.2006.11.030
[16] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 8(6), 1259–1284. https://doi.org/10.1142/S021812749800098X
[17] Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022
[18] Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals, 35(2), 408–419. https://doi.org/10.1016/j.chaos.2006.05.064
[19] Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimensional chaotic system. Optics Communications, 284(16–17), 3895–3903. https://doi.org/10.1016/j.optcom.2011.04.030
[20] Patidar, V., Pareek, N. K., & Sud, K. K. (2011). A new substitution–diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 16(1), 368–382. https://doi.org/10.1016/j.cnsns.2010.04.016
[21] Tong, X., & Cui, M. (2008). Image encryption scheme based on fractional-order hyperchaotic system. Optics and Lasers in Engineering, 46(4), 336–342. https://doi.org/10.1016/j.optlaseng.2007.09.004
[22] Zhang, Y., & Wang, X. (2010). An image encryption algorithm based on DNA encoding and chaotic maps. IEEE Transactions on Circuits and Systems for Video Technology, 18(6), 885–890. https://doi.org/10.1109/TCSVT.2008.918826
[23] Li, S., & Mou, X. (2004). Security analysis of chaotic encryption schemes. Physics Letters A, 298(2–3), 131–137. https://doi.org/10.1016/j.physleta.2002.08.048
[24] Abdel-Aty, M., & Obada, A.-S. F. (2003). Quantum encryption based on chaotic maps. Physics Letters A, 309(4–5), 221–228. https://doi.org/10.1016/S0375-9601(03)00159-5
[25] Kaur, M., & Singh, S. (2018). A novel hybrid approach for image encryption using quantum logistic map and DNA sequence operation. Multimedia Tools and Applications, 77(24), 31913–31936. https://doi.org/10.1007/s11042-018-6108-4

[26] Zhang, W., & Wang, X. (2013). A novel image encryption scheme based on quantum logistic map. Quantum Information Processing, 12(2), 739–753. https://doi.org/10.1007/s11128-012-0405-8
[27] Wu, Y., Noonan, J. P., & Agaian, S. (2012). Image encryption using quantum chaotic systems. Optics and Lasers in Engineering, 50(12), 1758–1768. https://doi.org/10.1016/j.optlaseng.2012.06.013
[28] Fang, L., & Wang, Z. (2017). Self-adaptive quantum chaotic image encryption algorithm. Optik, 131, 1321–1330. https://doi.org/10.1016/j.ijleo.2016.12.013
[29] Singh, P., & Mandal, S. (2017). A survey on image encryption techniques. Journal of Network and Computer Applications, 78, 35–46. https://doi.org/10.1016/j.jnca.2016.11.013
[30] Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm. Optics and Lasers in Engineering, 56, 83–93. https://doi.org/10.1016/j.optlaseng.2013.12.010
[31] Zhu, C., Sun, K., & Wang, S. (2017). A chaos-based image encryption scheme using permutation and DNA encoding. Optik, 140, 1347–1358. https://doi.org/10.1016/j.ijleo.2017.03.065
[32] Wang, X., Zhang, L., & Guo, Y. (2019). A survey of chaotic image encryption algorithms. Mathematical Problems in Engineering, 2019, 1–16. https://doi.org/10.1155/2019/3731852
[33] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926–934. https://doi.org/10.1016/j.imavis.2006.02.021
[34] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 8(6), 1259–1284. https://doi.org/10.1142/S021812749800098X
[35] Patidar, V., Pareek, N. K., Sud, K. K., & Nagar, A. K. (2009). A robust and secure chaotic standard map based pseudorandom permutation–substitution image encryption. Optics Communications, 284(19), 4331–4339. https://doi.org/10.1016/j.optcom.2009.06.063
[36] Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022