IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 43-51
Journal homepage: http://iieta.org/journals/ijsse

Biometric Data Encryption Using a New Five Dimensional Hyper-Chaotic System

Maryam T. M. Alghamazi*, Sadiq A. Mehdi, Emad I. Abdul Kareem

Department of Computer Science, College of Education, Mustansiriyah University, Baghdad 10001, Iraq

Corresponding Author Email: maryam_alghamazi@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.150105

Received: 17 November 2024
Revised: 29 November 2024
Accepted: 15 January 2025
Available online: 31 January 2025

Keywords:
biometric data, 5-D hyper-chaotic, image encrypting, diffusion, confusion, security analysis, sensitivity to initial conditions

ABSTRACT

Interest in the biometric data has significantly increased as a result of its potential as one of the reliable methods of authentication. To provide safe storage and transmission of the biometric data images over the public networks, a fast and lossless cryptosystem is highly necessary. The present study introduces a new approach for biometric image encryption with the use of a hyper-chaotic map. A hyper-5D chaotic system has been suggested as a solution for diffusion and confusion problems, with the added advantage of providing a vast key space. This method is heavily dependent upon the chaotic sequences that are produced through the chaotic system in 5-D. A strong level of encryption is ensured with the use of such sequences for the modification and reorganization of pixel values through the image. The proposed system's effectiveness has been evaluated with the use of several performance measures from the security analysis. These included key space analysis, key sensitivity analysis, histogram analysis, correlation coefficient, peak signal-to-noise ratio (PSNR), unified average changing intensity (UACI), information entropy, mean square error (MSE), and time efficiency analysis. The strengths of the suggested cryptosystem against brute force, differential, and statistical attacks have been confirmed by the security analysis findings.

1. INTRODUCTION

A new age has started with the widespread deployment of biometric technology, which uses features for identification [1]. Facial identification, fingerprint analysis, iris scanning, ear morphology, and palm print patterns are prominent. Biometric technologies are popular because of their cost-effectiveness, accuracy, and user acceptance [2, 3]. Biometric identity is used in almost all digital media, including mobile phones, computers, attendance systems, and special areas that need fingerprints, iris patterns, and palm prints. To protect biometric images sent and stored over public networks, a quick, lossless, and secure cryptographic solution is needed. Since its 1970s introduction, chaos theory has influenced several areas. These areas include engineering, math, biology, and physics [4]. Lorenz [5] introduced chaos theory into various sciences. Chaos maps are crucial to cryptography because their characteristics match avalanche, balance, diffusion, and confusion [6]. Chaotic maps are ideal for creating secure and complex encryption methods, making them resistant to cryptographic attacks.

This study identifies the hyper-chaotic maps as one of the new techniques of encryption for the protection of the biometric images. The novel approach utilizes a chaotic system consisting of 5 differential equations, which generates chaotic sequences for each dimension. Such sequences ensure that the encrypted image is extremely resistant to attacks and cannot be recognized through changing and hiding the pixel values of the input image. The procedure starts by creating chaotic sequences according to a set of system parameters and beginning conditions.

After applying these sequences to the input image, non-zero pixels are saved in a different array for additional processing, while zero-valued pixels are immediately replaced with chaotic values.

The non-zero pixels are then shuffled using the chaotic sequences that were produced. Scrambling the locations of pixels eliminates the correlation between neighboring pixels, making it harder for unauthorized individuals to extract valuable information from the image. The technique includes an XOR operation between chaotic sequences and the pixel values along with chaotic permutation.

In order to guarantee that even minor modifications to the original image produce a substantially different encrypted output, this stage further diffuses the pixel information. The image is then separated into small blocks, usually 8 by 8 pixels, and a dynamic S-box is used to perform a substitution procedure on each block. The chaotic system creates the S-box, which is frequently moved to maintain a high degree of security and randomness. The method of decryption is the opposite of the algorithm used for encryption.

This restores the original image by undoing the scrambling and substitution processes using the same chaotic system, keys, and initial conditions. Because of the chaotic system's high sensitivity, even a small change in the key or beginning conditions will prevent decryption, making the system extremely safe from standard attacks like brute-force.

The study's next sections are structured as follows: An overview of related work is given in Section 2. The relation between cryptography systems and chaos systems is described in Section 3. A brief synopsis of the chaotic system is provided in Section 4. The details of the suggested scheme are described in Section 5. An analysis and discussion of the experimental findings are presented in Section 5. The final section presents conclusions and suggestions for future work.

2. RELATED WORKS

In computing, chaos-based methods have proven to perform better in terms of security, speed, and complexity. These days, cryptographic methods depending on chaos are suggested for innovative security uses. It is possible to divide chaos-based encryption into two main categories [7]: asymmetric and symmetric. Most symmetric chaos-based approaches are formulated in terms of discrete chaotic maps. The use of chaotic dynamics in cryptography is done using two different methods. The first "stream ciphers" obscure plaintext using a variety of techniques that use key streams and chaotic systems to produce pseudo-random sequences. In the second method, known as "block ciphers," the cipher is derived from the initial state orbit that the plaintext established [8].

A novel technique for digital fingerprint image encryption is illustrated in the work that has been presented in previous study [9]. The technique encodes the image using DNA sequencing and the chaotic tent map. Both the initial image as well as the chaotic mapping are individually encrypted by DNA sequencing. After that, the logical XOR operator is used, which creates the encrypted image by using chaotic systems. The chaotic tent map can only work with one input value at a time, which limits its ability to build complex, high-dimensional chaotic patterns that could provide more security. The tent map's low dimensionality makes it easier for attackers to predict or evaluate chaotic behavior than higher-dimensional chaotic systems.

Using hybrid chaotic maps, a new encryption technique for palm print image protection was presented in previous study [7]. In addition to providing a significant key space, the proposed hybrid method aims to address the challenges of misunderstanding and dispersion. For a certain set of the control settings, this method combines a variety of the chaos map. Integrating many chaotic maps into one hybrid system could provide significant technical obstacles. It may get much trickier as there's a need to maintain the maps updated and prevent unexpected behavior that can impair performance.

Another example of creative efforts is a study of Hashad et al. [10], which presented a method of encryption for the fingerprint images. This method presents a reliable mechanism for the protection of fingerprint data with the use of the chaotic Baker map, well-known due to having a remarkable resilience to the signal noise. The approach is tested for fingerprint images, but it may struggle to scale for huge biometric databases. In large-scale biometric systems, managing encrypted biometric templates and executing encryption/decryption procedures may become problematic as user enrollment increases.

Through the use of the dual-beam interference and the chaotic maps, a unique optical authentication technique has been presented for the purpose of providing a fresh approach to the problems with biometric authentication [11]. The optical authentication technique based on two-beam interference might be sensitive to environmental factors such as lighting conditions and optical distortion, which can affect its reliability in real-world scenarios.

3. THE CONNECTION BETWEEN CHAOTIC SYSTEMS AND CRYPTOGRAPHIC SYSTEMS

British mathematician Matthews originally suggested an encryption method grounded on the logistic chaotic system in 1989. Since then, the area of cryptography has benefited from several chaotic systems. Fridrich presented the first chaos-based image encryption system in 1998 using two fundamental characteristics of a safe cipher: confusion and diffusion designs [12].

Chaos theory is vital in modern cryptography due to its inherent characteristics, including great sensitivity to initial conditions, topological mixing, and unpredictability. These features align with the essential characteristics of efficient ciphers, including confusion as well as diffusion [13, 14]. For example, in chaotic systems, sensitivity to starting points and system parameters is analogous to how cryptographic techniques are sensitive to plaintext and keys [15].

The long-term unpredictability of a chaotic system is characterized by its dependency on initial conditions. As a result, even a small variation between two initial conditions can lead to significant separation, and the assessed system will be unpredictable [16]. A topological mixing in a chaotic system is analogous to cryptography's uniform distribution function [17]. Understanding the link between chaos and cryptography is rather crucial; hence Table 1 demonstrates the characteristics of both systems [18, 19].

Table 1. Comparison of chaos with the characteristics of cryptography

Seq.	Cryptography Algorithms	Chaotic Characteristic	Explanation
1.	Diffusion	Extremely sensitive to both the initial conditions and the control parameters that were used.	A relatively minor variation in the input results in a significantly different output.
2.	Confusion	Ergodicity Mixing property Auto similarity	Regardless of the input, the system generates a similar output.
3.	Algorithmic Complexity	Complexity	Highly challenging outputs are generated by a straightforward algorithm.
4.	Deterministic	Pseudo randomness Deterministic	A pseudo randomness is generated by a deterministic procedure.

This table highlights how certain chaotic properties are analogous to important aspects of cryptographic functions. The chaotic characteristics provide a foundation for designing cryptographic algorithms that exhibit strong confusion, diffusion, pseudo-randomness, and complexity—key elements in secure encryption systems.

4. DEVELOPMENT OF A NEW FIVE-DIMENSIONAL DYNAMIC SYSTEM

By definition, a hyper-chaotic system is one that has two or more positive Lyapunov exponents [20]. It implies that the system's chaotic dynamics are amplified in multiple directions, resulting in the formation of more complex attractors [21]. The main aim is improving a mathematical model incorporating a new chaotic cipher system. In order to obtain the new 5D autonomous system, users must complete these steps:

$$\begin{aligned}
\frac{dx_1}{dt} &= -a\,x_1 + b\,x_2 + c\,x_3x_4 - \,x_3x_5 \\
\frac{dx_2}{dt} &= -\,x_2 + d\,x_1 - e\,x_1x_3 - f x_5 \\
\frac{dx_3}{dt} &= -g\,x_3 + f\,x_1x_2 + x_4 \\
\frac{dx_4}{dt} &= -h\,x_4 - i\,x_1x_3 + j\,x_5 \\
\frac{dx_5}{dt} &= -b\,x_5 + a\,x_2x_3 - x_1x_3
\end{aligned} \tag{1}$$

where, *a*, *b*, *c*, *d*, *e*, *f*, *g*, *h*, *i*, and *j* are the system's positive parameters. The current state of the system is represented by x_1, x_2, x_3, x_4, and x_5.

The recently constructed 5D system (1) displays a chaotic attractor when the parameters selection conditions are as follows: *a*=5, *b*=3, *c*=3.50, *d*=20, *e*=2.20, *f*=0.50, *g*=4.50, *h*=0.80, *i*=2.30, and *j*=1.20.

The specified starting conditions are: $x_1(0)=0.10$, $x_2(0)=0.30$, $x_3(0)=0.4$, $x_4(0)=0$, $x_5(0)= 0.01$.

This system had exhibited a broad range of the complicated and unpredictable chaotic behaviors.

Figures 1 and 2 illustrate the attractors in three-dimensional and two-dimensional representations. The structure mimics the bow of a ship, giving rise to the term "Butterfly Effect".

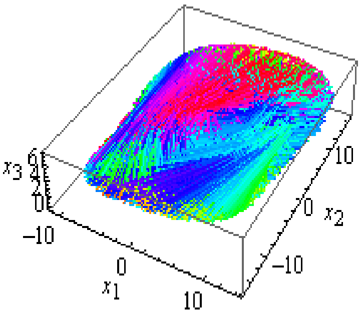


Figure 1. Representation of chaotic attractor points in three dimensions (x_1, x_2, x_3)

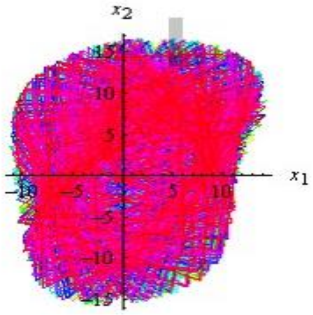


Figure 2. Chaotic attractors, (x_1–x_2) phase plane

4.1 Lyapunov dimensions and Lyapunov exponents

In accordance with the principles of nonlinear dynamical theory, the Lyapunov exponent is determined by use of a quantitative measure technique that is very dependent on the initial conditions. Essentially, it's the average rate at which two close trajectories are moving in opposite directions [22, 23]. Furthermore, the five Lyapunov exponents with parameters for the nonlinear dynamical system (1) are as follows: a=5, b=3, c=3.5, d=20, e=2.2, f=0.5, g=4.5, h=0.8, i=2.3, and j=1.2, and obtained in the subsequent manner:

LE1=4.03832, LE2=3.5148, LE3=6.85408, LE4=-5.89531, LE5=-22.8248. As observed, since the largest Lyapunov exponent is positive, the system displays chaotic characteristics. There are three positive Lyapunov exponents (LE1, LE2, and LE3) and two negative ones.

5. THE EFFICIENT BIOMETRIC IMAGE ENCRYPTION METHOD

The suggested encryption algorithm includes many steps, starting with the initialization and then progressing through a variety of the techniques of diffusion and confusion. The process is heavily dependent upon using chaotic sequences that have been generated by a 5-D chaotic system. These sequences are utilized in order to change and rearrange values of pixels throughout the image for ensuring strong encryption. The structure of the suggested system is depicted in Figure 3.

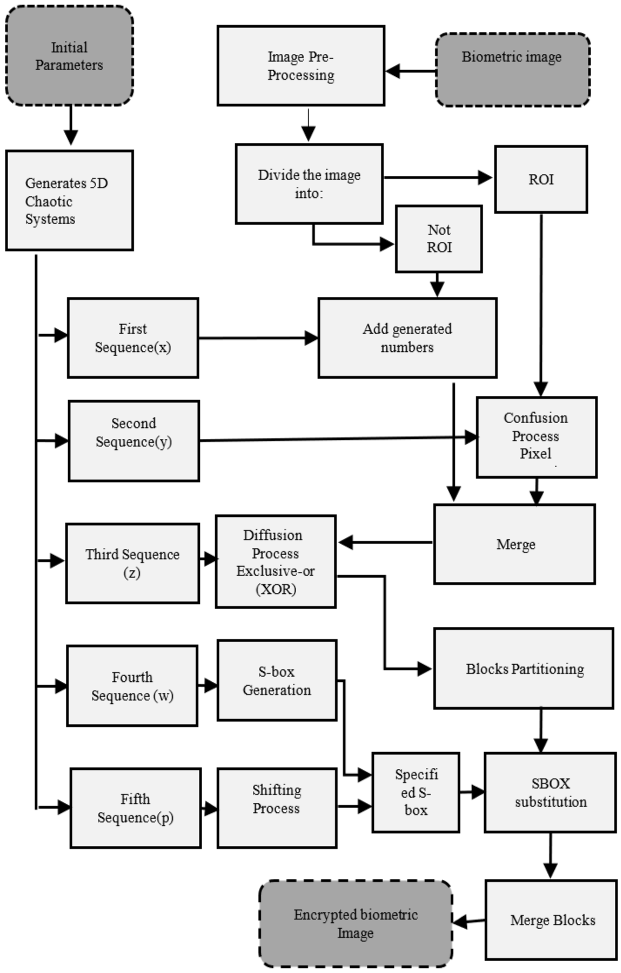


Figure 3. Layout for the suggested system

5.1 Algorithm steps

Step 1: Generation of the initial parameters and 5D chaotic system.

The first step of the algorithm is establishing starting parameters of the chaotic system. Five different chaotic sequences are produced from these starting conditions:

- First Sequence (x): Utilized for pixel value modification in Not ROI.
- Second Sequence (y): Handles the confusion process (pixel permutation) for Region of Interest (ROI).
- Third Sequence (z): Controls the diffusion process.
- Fourth Sequence (w): Responsible for the generation of the S-box that is utilized in the process of substitution.
- Fifth Sequence (p): Utilized in the shifting process for additional manipulation of the pixels.

Step 2: Initial image pre-processing.

The image is resized to an (n × n) matrix. The image is separated into two main parts after the pre-processing:

- ROI (Region of Interest): The most important area of the image, due to the fact that it includes significant structures.
- Not ROI: The less important parts that are not considered to have a big impact on the biometric identity.

Step 3: Pixel value addition (Not ROI).

The chaotic numbers that have been produced by the first sequence (x) are added to the values of the pixels for the Not ROI region, giving the process of encryption more robustness in general, by ensuring that even image parts of lower significance are changed.

Step 4: Confusion process.

Confusion (ROI): The Confusion process ensures that the pixel locations of ROI are permuted (shuffled) based on the second Sequence (y). This step adds another layer of complexity by ensuring that the arrangement of pixels is scrambled.

Step 5: Merging of ROI (Not ROI).

The image is reassembled, where ROI and Not ROI regions are integrated into a unified image after the processes of confusion and pixel value addition are independently performed for every section.

Step 6: Diffusion process.

Pixel values of the image are XORed with the chaotic numbers by using the 3rd (z) chaotic sequence, which is done in order to ensure that even little adjustments to the key or the input image lead to noticeable changes to the encrypted image.

Step 7: Partitioning images into blocks.

The image is further partitioned into (n×n) non-overlapping blocks, with each block being further encrypted utilizing a substitution box (S-box) derived from the chaotic map.

Step 8: S-box Generation.

The fourth chaotic sequence (w) is used to create a substitution box (S-box), which is organized into a (16×16) matrix. S-boxes are essential parts of cryptographic algorithms; they increase data security through non-linear mappings by replacing the values of input data with output values.

Step 9: Shifting process.

An extra layer of security is added by shifting the S-box with the use of a chaotic number from the Fifth Sequence (p). The shifted S-box is used to encrypt each block, guaranteeing diffusion over the image. This procedure mitigates the effects of assaults such as differential cryptography, in addition to improving the encryption.

Step 10: Merging blocks.

Blocks are combined back into a single image after they have all been encrypted.

Step 11: Final encrypted image.

Due to the utilized chaotic transformations, the final output represents an encrypted biometric image ready to be safely transmitted or stored and shows significant resistance to the attacks.

5.2 Decryption image

The process of decryption can be simply described as the opposite of encryption, and the proposed technique of encryption is symmetric. For the purpose of precisely restoring the original biometric image, the processes of encryption have to be reversed throughout the process of decryption. Initially, the encrypted image is split into N×N blocks, and an inverse S-box transformation has been used for the decryption of every block. This reverse substitution undoes pixel confusion and diffusion that have been applied throughout the process of encryption, making sure that pixel values are recovered accurately. After the decryption of every block, they're reassembled in order to reconstruct the full image.

One more XOR operation is carried out with the chaotic sequence that has been utilized throughout the process of encryption, which is helpful in the full retrieval of pixel values. The masked regions, which represent regions of interest (ROI), are processed in a separate manner for the purpose of ensuring that only relevant image portions are decrypted. The decryption accurately restores the biometric image through the re-ordering and decryption of pixels in ROI based upon their original positions. Finally, the decrypted image is saved and then verified visually for the purpose of ensuring that it matches the original image before the encryption. This robust multi-step method of decryption ensures the security as well as the integrity of biometric data, which makes it suitable for the sensitive types of applications.

6. SECURITY ANALYSIS

For the evaluation of the quality of the encryption algorithm, a statistical analysis is performed. The utilized performance metrics include key space analysis, key sensitivity analysis, histogram analysis, correlation coefficient, number of pixels change rate (NPCR), unified average changing intensity (UACI), peak signal-to-noise ratio (PSNR), mean square error (MSE), information entropy, and time efficiency analysis.

6.1 Key space analysis

The total number of distinct keys available for use in the encryption process is indicated by the key space size. There must be sensitivity to the secret keys in an effective encryption scheme. If the key space is too small, brute force attacks can be carried out. A smaller key space is typically associated with a more susceptible attack method.

From a cryptographic standpoint, to render brute force assaults ineffective, the key space must be a minimum of 2^{128} [24]. The key space size can reach around $(10^{14})^{15} = 10^{210} \simeq 2^{693}$, so exceeding$2^{128}$. The key area has been enough sized to endure brute-force fatigue assaults.

6.2 Key sensitivity analysis

An attack that attempts to determine the actual key by thoroughly predicting every potential combination is known as a brute force attack. Key sensitivity measures how resilient a cryptographic system is against this kind of attack. The cryptographic approach can endure 10^{14} possible key combinations before an attacker is likely to locate the proper key, as indicated by its key sensitivity of 10^{14}. The privacy of images across several apps may be assured with this degree of key sensitivity, which is strong.

6.3 Histogram analysis

Completely removing any statistical link between the encrypted and original images is required to avoid the extraction of important information from the unencrypted image and to protect against statistical attacks. The histogram regarding the encrypted image should be entirely flat and easily differentiated from the original image's histogram in order to be deemed encrypted [24]. The histograms of the encrypted and original images are displayed in Table 2 (a, b, c). It shows that the distribution is entirely random and constant across the whole image range. The strong encryption scheme, as well as the successful diffusion stage in the proposed approach, results in a completely new and uniform histogram for the encrypted image.

6.4 Analysis of the correlation coefficient

Analyzing the correlation coefficients shows that all of the pixels in a plain image are closely related to each other, regardless of whether they are horizontally, vertically, or diagonally arranged [25].

The values of the correlation between adjacent pixels in the horizontal (H), vertical (V), and diagonal (D) orientations are displayed in Table 3. While the encrypted image shows reduced correlation values, the unencrypted image shows strong correlation in all directions.

Table 2(a). The original, encrypted, decrypted biometric images produced by the proposed system (palm-print and iris images)

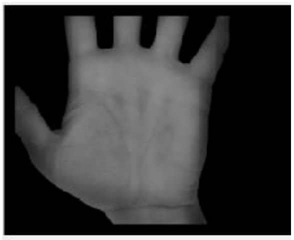
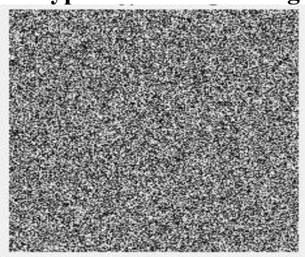
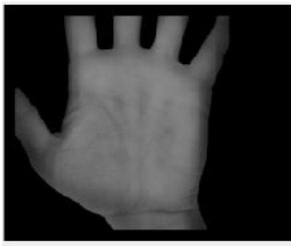
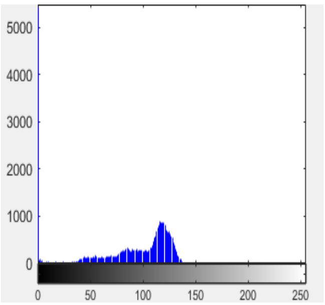
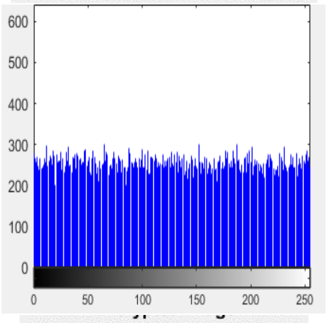
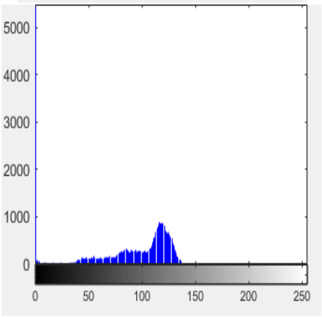
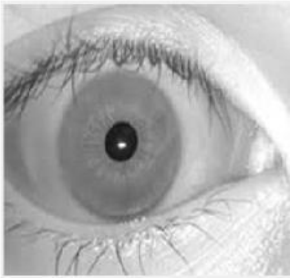
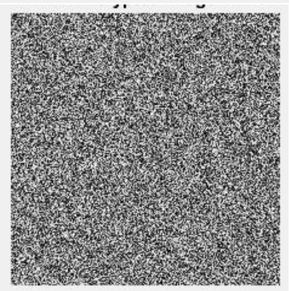
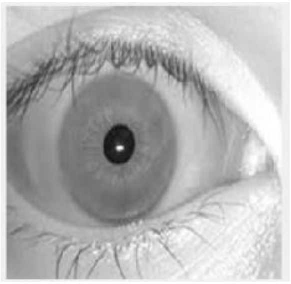
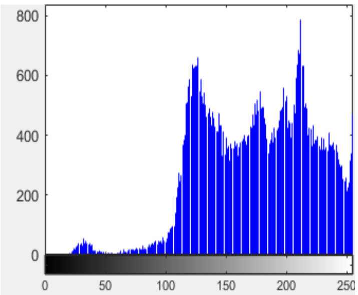
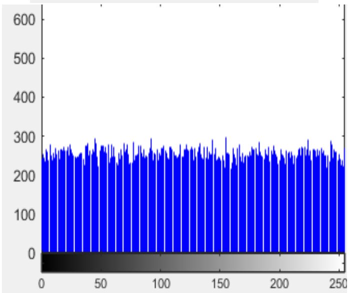
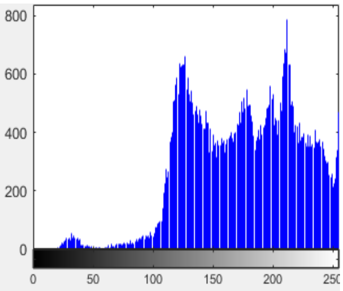
Original Biometric Image	Encrypted Biometric Image	Decrypted Biometric Image
		
		
		
		

Table 2(b). The original, encrypted, decrypted biometric image produced by the proposed system (Face image 1)

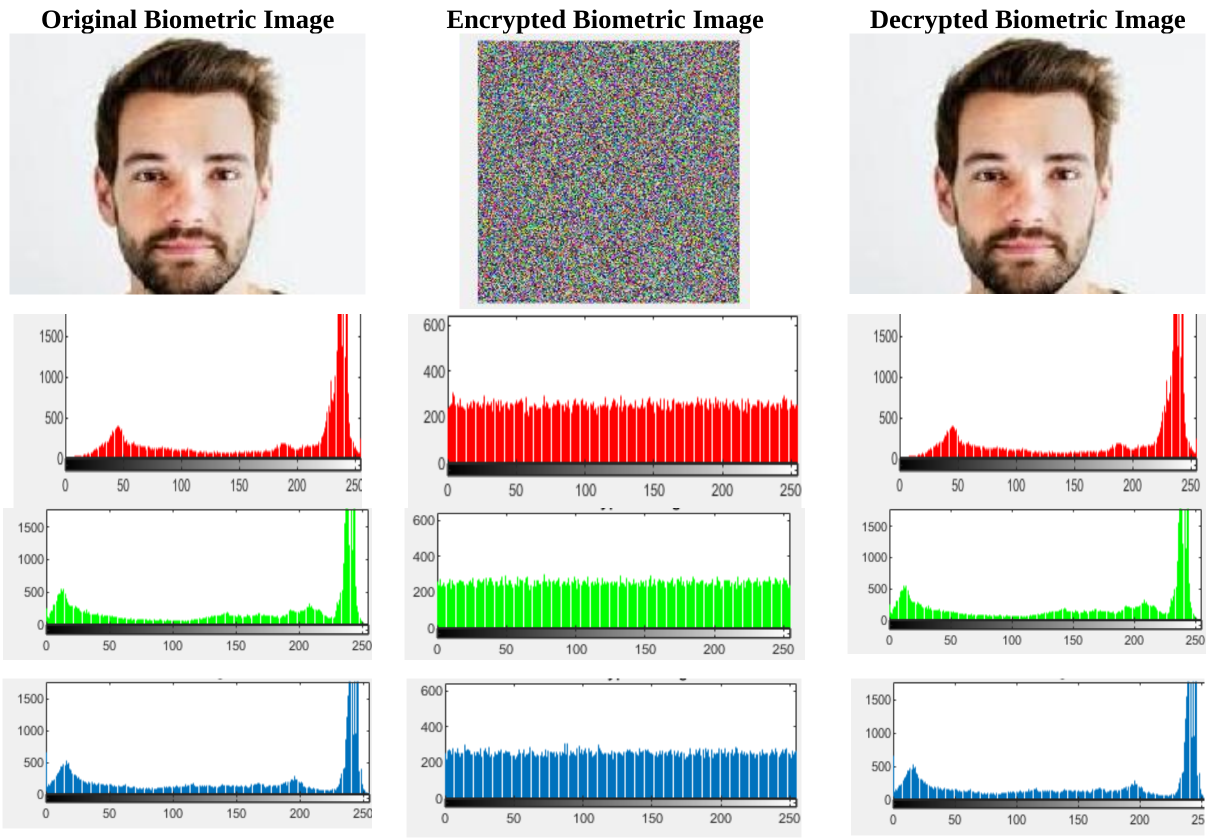


Table 2(c). The original, encrypted, decrypted biometric image produced by the proposed system (Face image 2)

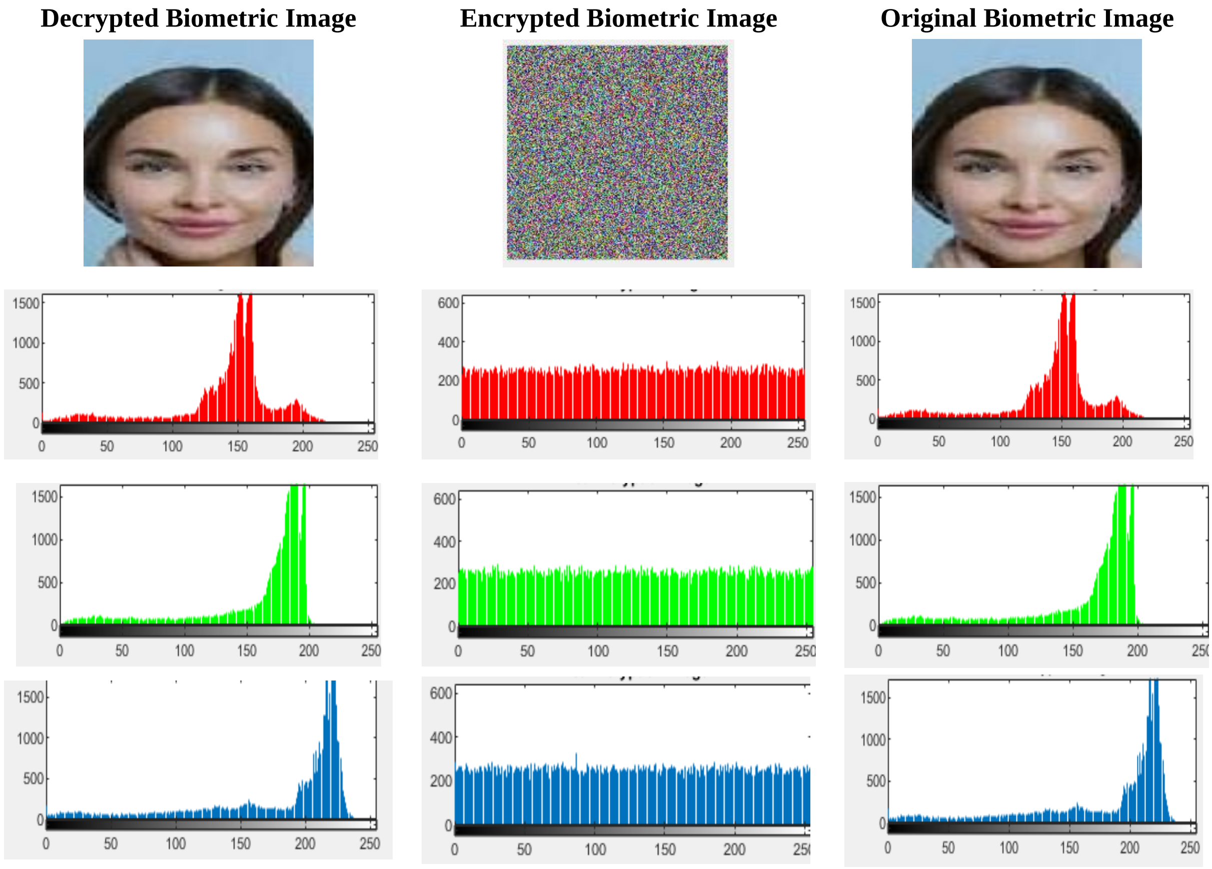
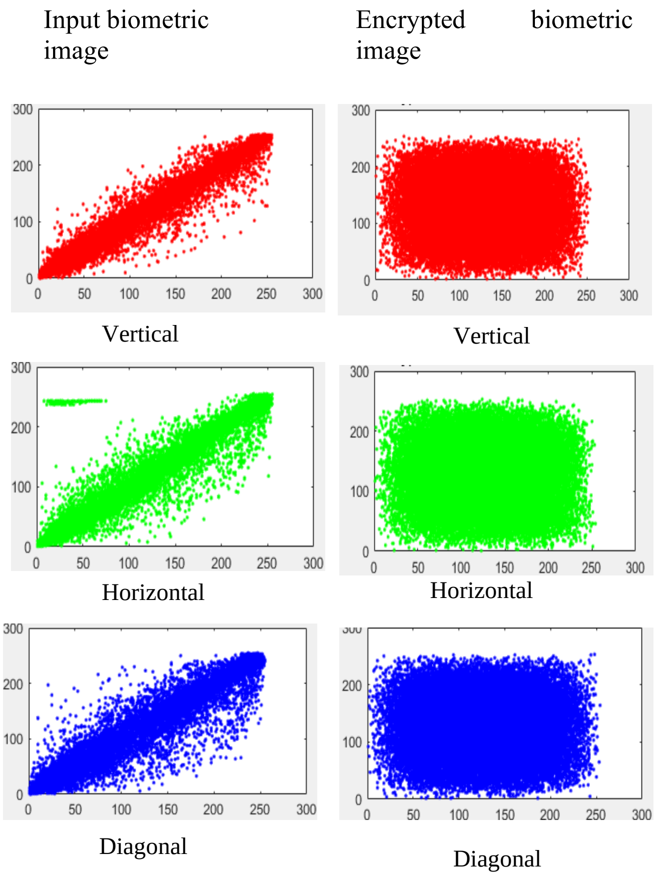


Table 3. Comparison of original and encrypted images by correlation analysis

Biometric Images	Correlation Coefficient for Input Biometric Images			Correlation Coefficient for Encrypted Biometric Images		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Palm-print image	0.9954	0.9969	0.9932	0.0038	0.0034	9.3202e-04
Iris image	0.9867	0.9905	0.9783	-0.0042	-0.0122	0.0068
Face image 1	0.9924	0.9781	0.9883	-0.0115	-0.0181	-0.0012
Face image 2	0.9824	0.9826	0.9728	-0.0146	-0.0199	0.0027



Vertical

Vertical

Horizontal

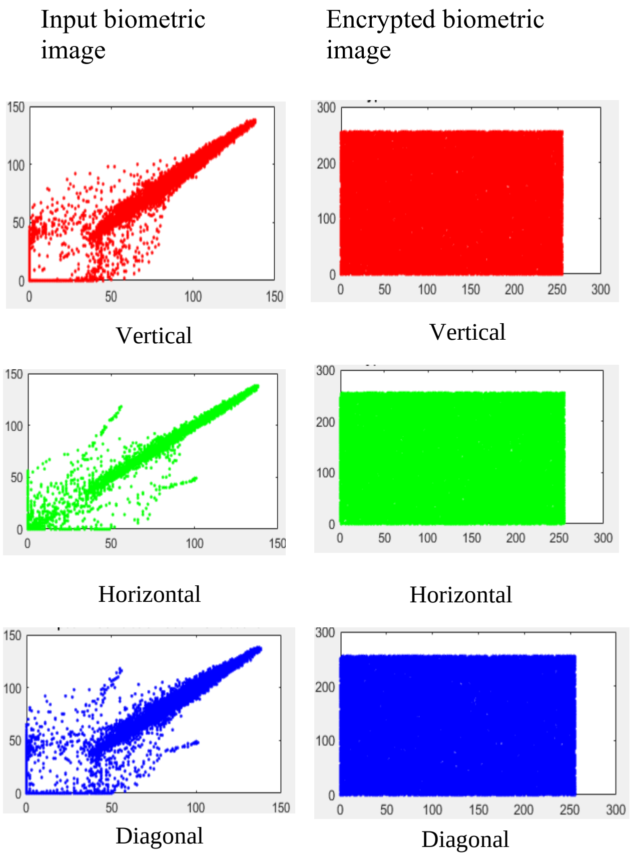
Horizontal

Diagonal

Diagonal

Figure 4. The vertical, horizontal, and diagonal correlations between two neighboring pixels in the input image and the encrypted image (Face image 1)

Figures 4 and 5 illustrate the horizontal, vertical, and diagonal correlation values between two neighboring pixels in the input image and the encrypted image. The correlation values reflect the resemblance between the original and encrypted images. The scatter plots demonstrate that the proposed encryption methods may produce encrypted images that are challenging to identify as the originals due to a poor connection. This indicates that the proposed encryption techniques adequately safeguard the privacy and confidentiality of images.



Vertical

Vertical

Horizontal

Horizontal

Diagonal

Diagonal

Figure 5. The correlation of two neighboring pixels in the input image and the encrypted image (palm-print image) in three different directions: vertically, horizontally, and diagonally

6.5 Occlusion attacks

Numerous encryption algorithms can be cracked by one important cryptanalyst technique known as the occlusion assault. Whole data blocks may be lost as a result of this type of attack, which taints a sent cipher image. The MSE and the PSNR are two important metrics that will be utilized to evaluate the system's resistance to occlusion attacks. PSNR is frequently regarded as one of the most crucial elements in the evaluation of image encoding quality due to the fact that it calculates the signal-to-noise ratio between two images [26].

A lower PSNR number between two images indicates a higher level of encryption quality.

Another important statistic used for the assessment of the efficacy of the proposed method is MSE, which shows the total amount of square error between two images. A higher MSE value suggests a better encryption outcome [27].

The MSE and PSNR values for the proposed system are displayed in Table 4. The suggested system exhibits exceptional performance for image decryption metrics, achieving zero MSE values and infinite PSNR values across all evaluated images, indicating its appropriateness for applications necessitating high-quality image decryption.

6.6 Entropy

The degree of unpredictability and randomness in the source data is indicated by the information entropy of the encrypted image. An attacker can decrypt an encrypted image if its entropy value is low.

Shanon's theory states that the optimal image entropy (H) is about 8 [28].

The entropy values of the original, encrypted, and decrypted images using the recommended encryption approach are shown in Table 5.

Table 4. The results of PSNR and MSE produced by the suggested system

Biometric Images	PSNR and MSE Values Between the Original and the Encrypted Image		PSNR and MSE Values Between the Original and the Decrypted Image	
	MSE	PSNR	MSE	PSNR
Palm-print image	14870.1296	6.4077	0	∞
Iris image	9871.0707	8.1872	0	∞
Face image1	14739.8047	6.4077	0	∞
Face image2	9366.1365	8.4152	0	∞

Table 5. Exhibits the entropy values of the original, encrypted, and decrypted images

Biometric Image	Entropy for Input Images	Entropy for Encrypted Images	Entropy for Decrypted Images
Palm-print image	4.0168	7.9963	4.0168
Iris image	7.3491	7.9957	7.3491
Face image1	6.9187	7.9989	6.9187
Face image2	7.104	7.999	7.104

6.7 Time efficiency analysis

It is crucial to consider the time factor when designing an encryption algorithm. An encryption algorithm that is more efficient in terms of sustaining its security level will be more effective when the execution time is reduced.

The experimental simulations were conducted on the MATLAB2023 platform with the following operating environment: an 8GHz Intel(R) Core (TM) i7-8550U CPU operating at 1.80GHz to 2.00GHz and a Windows 10 operating system. The efficiency performance of the proposed system is evaluated by calculating the time required for encryption and decryption procedures in seconds. The duration values for various biometric images are presented in Table 6.

Table 6. The results of the time spent encrypting and decrypting the image

Biometric Images	Encryption Time in Seconds	Decryption Time in Seconds
Palm-print image	0.1290	0.3622
Iris image	0.1985	0.3611
Face image1	1.3055	0.3695
Face image2	1.0769	0.3218

7. CONCLUSIONS

In the presented study, a new biometric image encryption approach depending on a 5D hyper-chaotic system is presented. This technique could be used for both the decryption and encryption of biometric images. The suggested encryption method, founded on a specialized hyper-chaotic system, demonstrates enhanced security against differential and statistical attacks due to its strong encryption capabilities, extensive key space, and resilience to statistical assaults, as evidenced by the experimental findings. The effectiveness of the current encryption method could be summed up as follows, with other benefits gained from the analytical tests carried out:

1. It is feasible to quantify the new five-dimensional chaotic system as hyper-chaotic due to its three positive Lyapunov exponents.
2. The suggested algorithm's large key space and ability to thwart brute-force attacks make it less vulnerable against a variety of attacks.
3. The coded algorithm's histogram is relatively flat, and correlation values between adjacent pixels are negligible and near zero, while the entropy is close to ideal value (8), proving the scheme's resilience and its capacity to thwart statistical attacks.
4. Both the NPCR and UACI results align well with the theoretical predictions of UACI and NPCR. Therefore, it is feasible to assume that the suggested encryption technique is robust enough to resist differential assaults.
5. PSNR values between test images and their respective encrypted images are infinite, whereas MSE between plain and decrypted images is zero.
6. The recommended method is both efficient as well as secure because of its short encryption and decryption times and its suitability for real-time transactions.

8. FUTURE WORK RECOMMENDATIONS

1. Embracing the innovative chaotic system in a new cryptographic method with improved security. For instance, the 5D hyper-chaotic may be implemented in future cryptography frameworks.
2. Employing higher-dimensional chaotic systems exceeding 5-D to augment the key space and enhance the chaos within the encryption system. The current work uses a 5D system, but further research should explore systems with more dimensions. Higher-dimensional chaotic systems (6D, 7D, or beyond) increase key space and chaos, making them more resistant to brute-force attacks.
3. Utilizing the encryption technique to secure other components such as audio or video. The existing encryption method has shown promise in safeguarding biometric images, but it might also be utilized for audio and video. Voice and video conferencing may be protected against eavesdropping and tampering with 5D hyper-chaotic encryption.

REFERENCES

[1] Qi, C., Li, M., Wang, Q., Zhang, H., Xing, J., Gao, Z., Zhang, H. (2018). Facial expressions recognition based on cognition and mapped binary patterns. IEEE Access, 6: 18795-18803. https://doi.org/10.1109/ACCESS.2018.2816044

[2] Dargan, S., Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143: 113114. https://doi.org/10.1016/j.eswa.2019.113114

[3] Nguyen, D.T., Pham, T.D., Batchuluun, G., Noh, K.J., Park, K.R. (2020). Presentation attack face image generation based on a deep generative adversarial network. Sensors, 20(7): 1810. https://doi.org/10.3390/s20071810

[4] El-Shafai, W., El-Mesady, A., Kamal, F.M. (2024). Enhancing biometric authentication security through the novel integration of graph theory encryption and chaotic logistic mapping. Multimedia Tools and Applications, pp. 1-35. https://doi.org/10.1007/s11042-024-19693-9

[5] Zolfaghari, B., Koshiba, T. (2022). Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap. Applied System Innovation, 5(3): 57. https://doi.org/10.3390/asi5030057

[6] Teh, J.S., Alawida, M., Sii, Y.C. (2020). Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications, 50: 102421. https://doi.org/10.1016/j.jisa.2019.102421

[7] Hikal, N.A., Eid, M.M. (2020). A new approach for palmprint image encryption based on hybrid chaotic maps. Journal of King Saud University-Computer and Information Sciences, 32(7): 870-882. https://doi.org/10.1016/j.jksuci.2018.09.006

[8] Fang, D., Sun, S. (2018). A new scheme for image steganography based on hyperchaotic map and DNA sequence. Journal of Information Hiding and Multimedia Signal Processing, 9(2): 392-399.

[9] Nezhad, S.Y.D., Safdarian, N., Zadeh, S.A.H. (2020). New method for fingerprint images encryption using DNA sequence and chaotic tent map. Optik, 224: 165661. https://doi.org/10.1016/j.ijleo.2020.165661

[10] Hashad, F.G., Zahran, O., El-Rabaie, E.S.M., Elashry, I.F., Abd El-Samie, F.E. (2019). Fusion-based encryption scheme for cancelable fingerprint recognition. Multimedia Tools and Applications, 78: 27351-27381. https://doi.org/10.1007/s11042-019-7580-x

[11] Souza, D., Burlamaqui, A., Souza Filho, G. (2018). Improving biometrics authentication with a multi-factor approach based on optical interference and chaotic maps. Multimedia Tools and Applications, 77: 2013-2032. https://doi.org/10.1007/s11042-017-4374-x

[12] Gopalakrishnan, T., Ramakrishnan, S. (2016). Image encryption in block-wise with multiple chaotic maps for permutation and diffusion. ICTACT Journal on Image & Video Processing, 6(3): 1220-1227. https://doi.org/10.21917/ijivp.2016.0177

[13] Shakir, H.R., Mehdi, S.A.A., Hattab, A.A. (2022). A dynamic S-box generation based on a hybrid method of new chaotic system and DNA computing. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(6): 1230-1238. https://doi.org/10.12928/telkomnika.v20i6.23449

[14] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2021). Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system. In Journal of Physics: Conference Series, 1804(1): 012048. https://doi.org/10.1088/1742-6596/1804/1/012048

[15] Biswas, H.R., Hasan, M.M., Bala, S.K. (2018). Chaos theory and its applications in our real life. Barishal University Journal Part, 1(5): 123-140.

[16] Mohammed, S.J., Mehdi, S.A. (2020). Web application authentication using ZKP and novel 6D chaotic system. Indonesian Journal of Electrical Engineering and Computer Science, 20(3): 1522-1529. https://doi.org/10.11591/ijeecs.v20.i3.pp1522-1529

[17] Bolotin, Y., Tur, A., Yanovsky, V. (2009). Chaos: Concepts, Control and Constructive Use. Berlin/Heidelberg, Germany: Springer. https://doi.org/10.1007/978-3-642-00937-2

[18] Tutueva, A.V., Nepomuceno, E.G., Karimov, A.I., Andreev, V.S., Butusov, D.N. (2020). Adaptive chaotic maps and their application to pseudo-random numbers generation. Chaos, Solitons & Fractals, 133: 109615. https://doi.org/10.1016/j.chaos.2020.109615

[19] Teh, J.S., Alawida, M., Sii, Y.C. (2020). Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications, 50: 102421. https://doi.org/10.1016/j.jisa.2019.102421

[20] Yu, F., Qian, S., Chen, X., Huang, Y., Cai, S., Jin, J., Du, S. (2021). Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map. Complexity, 2021(1): 6683284. https://doi.org/10.1155/2021/6683284

[21] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2020). Analysis of novel seven-dimension hyper chaotic by using SDIC and waveform. In 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), pp. 95-99. https://doi.org/10.1109/IICETA50496.2020.9318940

[22] Shakir, H.R., Mehdi, S.A., Hattab, A.A. (2023). A new four-dimensional hyper-chaotic system for image encryption. International Journal of Electrical and Computer Engineering, 13(2): 1744. https://doi.org/10.11591/ijece.v13i2.pp1744-1756

[23] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2021). Bifurcation of novel seven-dimension hyper chaotic system. In Journal of Physics: Conference Series, 1804(1): 012051. https://doi.org/10.1088/1742-6596/1804/1/012051

[24] Zhu, S., Zhu, C. (2018). Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system. Multimedia Tools and Applications, 77: 29119-29142. https://doi.org/10.1007/s11042-018-6078-2

[25] Jasem, N.N., Mehdi, S.A. (2023). Multiple random keys for image encryption based on sensitivity of a new 6D chaotic system. International Journal of Intelligent Engineering & Systems, 16(5): 576-585. https://doi.org/10.22266/ijies2023.1031.49

[26] Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Masood, F., Khan, F., Buchanan, W.J. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. IEEE Access, 8: 140876-140895. https://doi.org/10.1109/ACCESS.2020.3012912

[27] Rashed, A.A., Hussein, K.A. (2022). A lightweight image encryption algorithm based on elliptic curves and chaotic in parallel. In 2022 3rd Information Technology to Enhance e-learning and Other Application (IT-ELA), pp. 24-30. https://doi.org/10.1109/IT-ELA57378.2022.10107924

[28] Kuffi, E.A., Mehdi, S.A., Mansour, E.A. (2022). Color image encryption based on new integral transform SEE. In ournal of Physics: Conference Series, 2322(1): 012016. https://doi.org/10.1088/1742-6596/2322/1/012016