

Security Enhanced Personal Health Record Sharing Mechanism in a Cloud-Based System

Sreelatha K K¹, Adarsh K Ramesh², Adithya krishna V K³, Anusma A K⁴, Jayanth V⁵

¹Department of Electronics and Communication Engineering, College of Engineering Thalassery, APJ Abdul Kalam Technological University, Kerala, India

²Department of Electronics and Communication Engineering, College of Engineering Thalassery, APJ Abdul Kalam Technological University, Kerala, India

³Department of Electronics and Communication Engineering, College of Engineering Thalassery, APJ Abdul Kalam Technological University, Kerala, India

⁴Department of Electronics and Communication Engineering, College of Engineering Thalassery, APJ Abdul Kalam Technological University, Kerala, India

⁵Department of Electronics and Communication Engineering, College of Engineering Thalassery, APJ Abdul Kalam Technological University, Kerala, India

Abstract - In the medical industry, the gathering and analysis of medical records play a vital role in diagnosing illnesses. Medical diagnosis relies heavily on high-resolution images, which can be large and require significant storage space. Cloud storage offers a convenient and scalable solution for medical images, but it introduces security vulnerabilities. In a cyberattack, patient privacy could be compromised if medical data are not adequately protected. Traditional cryptographic methods encrypt medical records using complex mathematical algorithms and secret keys and store the encrypted data in a single storage space. These cryptographic methods protect the data from unauthorized access, introduce the complexity of managing keys, and are vulnerable to single-point attacks. Therefore, this paper proposes a novel, distributed Visual Secret sharing-based keyless algorithm to share medical records securely. The proposed framework uses random grid-based visual secret sharing and data hiding for efficient and secure transmission. Different security parameters such as SSIM (≈ 0), MSE (≈ 0), PSNR (≤ 8 dB), and entropy (≈ 8) show that the proposed method exhibits the highest level of security. Similarly, better reconstruction ability is evaluated using different human visual system parameters. Simulation results also show that the proposed work outperforms the existing techniques regarding reconstruction quality, better embedding rate, low operational complexity, and improved security.

Key Words: Security, Visual Secret Sharing (VSS), Medical Image Sharing (MIS), Reversible Data Hiding (RDH), Personal Health Record (PHR).

I. INTRODUCTION

A medical image is a visual representation of the interior of a body. It includes X-rays, CT scans, MRIs, and Ultrasounds. In health institutes, patients' records include all personal data, including text and images. In the event of a cyber attack, these data can be

compromised. The health sector has been dramatically impacted by modern technology. Various cures and diagnostics have been developed. The most significant among them is the various types of imagery used to diagnose any potential illness [1]. In most cases, they may be required to take an imagery test; in most cases, medical images become a large sizable portion of personal health records. All these data, including the medical images, are usually stored in a third-party cloud server for easy and timely access. Such files stored in a Third-party server carry potential risk in the event of a cyber attack [2]. Numerous data breaches have been reported across repositories recently, prompting researchers to develop various security frameworks in response to these medical data breaches.

Various cryptographic algorithms are employed [3]–[7], [18] to enhance the security of medical images. The effectiveness of these cryptographic algorithms hinges on the secrecy of the cryptographic key. If the secret key is exposed, it can render the cryptographic techniques susceptible to security attacks. Additionally, many cryptographic techniques store encrypted images (cipher images) in a centralized database, making them vulnerable to single-point attacks. To mitigate these challenges, this paper introduces a novel method by hiding personal text-based data into their respective personal medical images and then using a cryptographic scheme known as Visual Secret Sharing (VSS) with distributed storage has been proposed [8].

The conventional Visual Secret Sharing (VSS) technique is a cryptographic approach that converts visual information into secret shares, subsequently disseminating them across various servers. This method is intended for binary images, employing essential metrics to generate these shares. The generated secret shares can be combined to reconstruct the original secret image. While the conventional VSS method is recognized for its straightforwardness and security, it does have a limitation referred to as pixel expansion. The expansion of pixels leads to a reduction in the quality of the reconstructed image. As a result, this approach is not

appropriate for guaranteeing the security of medical images, where it is essential to uphold high-quality image reconstruction. Given that a majority of medical images are presented in grayscale, numerous Visual Secret Sharing methods employ halftoning techniques before the creation of shares. Halftoning converts grayscale images into binary format; however, this extra step raises pre-processing overhead and reduces the quality of the reconstructed image.

In response to these challenges, a new image cryptographic technique named Medical Image Sharing (MIS) using XOR-based VSS with improved contrast has been proposed. MIS offers a pixel expansion-free scheme, overcoming the limitations of traditional VSS methods. In addition, a data embedding scheme is also proposed to secure patient information. The contribution of this paper is summarized below.

- Proposed a VSS-based distributed security mechanism that completely avoids single-point attacks.
- PBTL-based data hiding is proposed to transfer the images and text data.
- Compared to existing data hiding methods, the proposed method provides secure data extraction. Secure means the algorithm requires all the n shares to reconstruct the embedded data.

The overall structure of the paper is organized in the following manner. The literature on VSS and RDH is detailed in Section II. The framework we propose is detailed in Section III. Section IV presents a comprehensive simulation and findings, followed by the conclusion in Section V.

II. RELATED WORK

A. Visual Secret Sharing

In conventional key-based cryptography, a secret key plays a crucial role in transforming a plain image (the original image) into a scrambled, unreadable form known as the cipher image. This key acts like a password for both encryption and decryption. The receiver needs the same secret key to decrypt the image and retrieve the original data. They use the decryption algorithm (basically the reverse encryption algorithm) and the key to unscramble the cipher image back into the plain image. The security of this approach relies heavily on keeping the secret key confidential. If someone manages to crack the key, they can decrypt the image and access its confidential information. The encrypted images within a standard cryptographic framework are consolidated in a singular database. This type of storage is vulnerable to attacks that target a single point. In order to address this challenge and improve security measures, VSS has been implemented.

Naor and Shamir introduced [9] a security scheme for visual data called VSS. VSS stands for Visual Secret Sharing. It is a cryptographic technique for securing visual data (like images or videos). VSS breaks down the original visual data into multiple secret shares (n shares).

Recovering the original data requires k number of shares ($((n, k)VSS)$). VSS offers advantages in complexity, key management, and security compared to cryptographic algorithms.

Chin et al. [10] propose a new method for visual secret sharing (VSS) called a self-verifying visual secret sharing scheme. This scheme allows for sharing secret images (grayscale or color) while ensuring verification, security, and efficiency. Chin et al.'s technique uses error diffusion, image clustering, interpolation, and inverse halftoning-based edge detection.

Yang and Lai [11] propose a new construction method for colored VSS. This method leverages existing black and white VSS approaches. Traditionally, VSS deals with black and white images. The secret is split into shares that look random but reveal the secret image when stacked together. This paper builds on existing black and white VSS schemes to create a method for sharing colored images.

"Improving the visual quality of random grid-based visual secret sharing" by Xiaotian Wu and Wei Sun [12] discusses a challenge in visual secret sharing (VSS) – the trade-off between image size and quality. The Random Grid Approach avoids pixel expansion by making each share the same size as the secret image. However, it sacrifices the visual quality of the revealed image.

T H Chen and K H Tsao [13] presented another random-grid-based (RGVSS) visual secret sharing to share secrets. Unlike traditional RGVSS, which uses confusing random patterns, this method creates shares incorporating a logo image. By analyzing this logo, users can recover the secret image when they stack the shares together. This approach offers two advantages: the shared images are the same size as the original secret, and they are easier to manage for users.

B. RDH

Reversible data hiding (RDH) hides information within digital images with a surprising twist, and it allows for the extraction of hidden data later and the perfect restoration of the original file. Unlike traditional methods, RDH keeps the original data pristine, making it ideal for sensitive applications like medical imaging. This innovative technique finds uses in copyright protection, content authentication, and secure medical data transmission.

Zhicheng et al. [14] propose a new method for reversible data hiding. This technique allows secret data to be embedded in an image (the cover image) so that the original image can be ideally recovered after the data is extracted. This paper proposes a novel RDH algorithm that utilizes the zero or minimum points in the image's histogram to embed data. The authors prove that the Peak signal-to-noise ratio (PSNR) between the original and marked image is guaranteed to be above 48 dB, significantly higher than previous techniques. A higher PSNR value indicates better visual quality.

Zhang [15] proposed a paper that discusses a reversible data hiding scheme for encrypted images.

Images are scrambled with a stream cipher, and extra data is embedded using spatial correlation. Two keys are needed to recover data and the original image: a decryption key and a data-hiding key. Hence, it allows secure data transmission as decryption only reveals a similar image, requiring both keys for full access.

The RDHEI method proposed by Yaomin et al. [16] addresses security concerns in AI and IIoT by allowing data hiding in encrypted images. It balances security with manageability using block-level encryption and reversible data-hiding techniques. The method achieves high embedding capacity and outperforms current methods, making it suitable for IIoT applications.

Tseng and Hsieh [17] propose a reversible data hiding method for images, ideal for applications like satellite or medical images where data integrity is paramount. The method hides data by modifying the difference between a pixel's value and its predicted value (based on neighboring pixels). Hence, this technique allows the user to embed more information in the image.

III. PROPOSED WORK

This section explains the structure of the proposed work. Figure 1 shows the workflow of the proposed work. The proposed work consists of two phases: 1. Text embedding and share generation, and 2. Personal Health Record reconstruction. In data embedding and share creation, the initial phase involves embedding private medical text data into images utilizing the data hiding approach. After data hiding, embedded images are transformed into n unique shares and kept across various databases. All generated shares are aggregated and overlaid during PHR reconstruction to recover the medical image. The incorporated medical textual data are derived from the associated medical image. A comprehensive explanation of each phase is shown below.

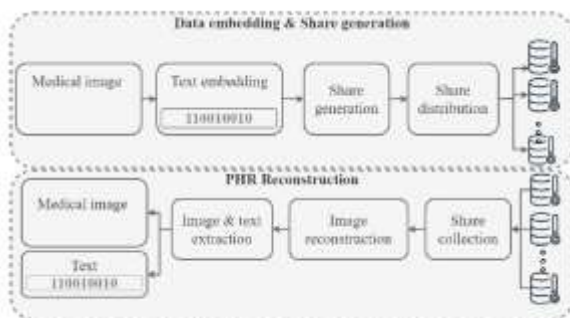


Fig –1: General block diagram of proposed work.

A. Data embedding & Share generation

This section consists of 2 phases: 1. Data embedding, and 2. Share generation and distribution.

1) Data embedding

Figure 2 depicts the workflow of data embedding. The Parametric Binary Tree Labelling (PBTL) framework embeds data into digital images while preserving their visual quality. The process involves four

main steps. Firstly, the original image is divided into smaller, non-overlapping blocks. Secondly, pixels within these blocks are grouped into categories: reference pixels, which remain unchanged; special pixels for storing parameters; embeddable pixels capable of hiding data; and non-embeddable pixels, which cannot hide data. Selecting reference pixels and categorizing the rest are based on predefined rules. Thirdly, pixels are labeled using PBTL (Pixel-Based Template Labelling), a method that assigns binary codes to non-reference and embeddable pixels. This labeling facilitates distinguishing pixel types and aids in later data extraction. Finally, the payload, comprising original pixel bits from particular pixels, replaced bits from non-embeddable pixels, and secret data, is embedded into the image. The remaining bits from embeddable pixels are utilized for this purpose. The framework also calculates the effective embedding rate considering the embedding capacity and constraints imposed by the parameters α and β , and determines the maximum embedding rate for various combinations of these parameters [19]. The detailed explanation for data embedding is explained in Algorithm 1.

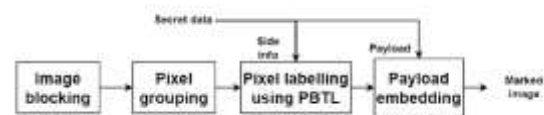


Fig –2: Framework of PBTL.

Algorithm 1 PBTL

Input: Medical image MI, Secret data SD, parameters α and β .

Divide MI into equal size non-overlapping blocks and classify pixels into four groups P_r , P_s , P_e , and P_n .

Construct the payload P , where it consists of the secret data M , the first β bits of each pixel in P_n , and 8 bits in P_s .

for each pixel in P_e do

 According to the difference value e , reconstruct the pixel by replacing α labeling bits and $(8 - \alpha)$ payload bits.

end for

for each pixel in P_n do

 Replace its first β bits by '0 ... 0 - β ' and keep the remaining $(8 - \beta)$ bits unmodified.

end for

Convert α and β into binary bits and store them into P_s by bit replacement.

Output: Marked image M_i .

2) Share generation

The output from Algorithm 1 is directed to the share generation block. Figure 3 illustrates the share generation process for a secret medical image denoted as MI_i . RG_1 through RG_n denote the generated shares. In this context, RG_1 through RG_{n-1} are produced utilizing the random number generation function, specifically through a coin flip mechanism. The RG_n is produced by executing the XOR operation on MI_i and all previously generated values from RG_1 to RG_{n-1} . Upon completion of the generation process for all n shares, the shares are subsequently transmitted to the share distribution module for the purpose of distributed storage.

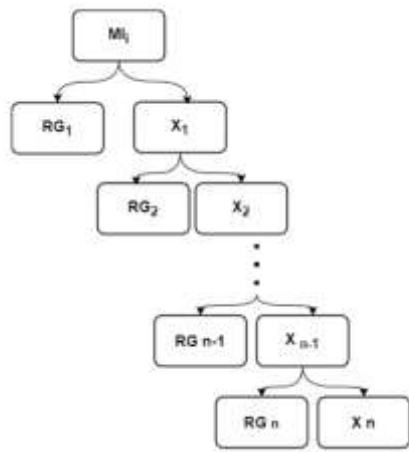


Fig. 3: Share generation & distribution

Fig –3: Share generation & distribution.

In Figure 3, each variable X_i is determined using Equation 1.

$$X_i = \{ M_i \oplus RG_i \text{ if } i = 1 ; X_{i-1} \oplus RG_i \text{ for } 2 \leq i \leq n - 2 \} \quad (1)$$

B. PHR reconstruction

After collecting all the shares from distinct databases, the embedded medical image is formed using logical XOR between all the shares. After reconstructing the embedded medical image, PBL-based data extraction is applied. The PBL data extraction process separates the image and data in a lossless manner.

IV. RESULT AND DISCUSSION

This section outlines various experiments conducted to evaluate the performance of the proposed method. Simulations were conducted using Python on a system equipped with an Intel i3 processor, 4GB of RAM, and a Windows 7 operating system. For comparison and evaluation purposes, all experiments are conducted with several shares n as three. Data hiding capacity is evaluated using random bits embedding in the image.

The entire results and discussion section is divided into two:

- Image quality and embedding rate
- Security analysis

Reconstructed image quality is evaluated using Human Visual System (HVS) parameters, and the embedding rate is evaluated using Bits Per Pixel (BPP). In security analysis, the quality of the generated shares is evaluated using the similarity between the generated shares and the original image. Fig. 4 shows the experimental results of (3,3)VSS system.

A. Image quality and embedding rate

Image quality is evaluated using various HVS parameters. The Structural Similarity Index (SSIM) assesses the similarity between two images by considering their luminance, contrast, and structure. It measures perceptual similarity rather than pixel-wise differences, making it robust to compression and noise. Peak Signal-to-Noise Ratio (PSNR) quantifies image

quality by comparing the peak signal strength to the noise level, with higher values indicating better quality. Normalized Cross-Correlation (NCC) evaluates how similar two signals are by measuring their correlation. Mean Squared Error (MSE) calculates the average squared difference between corresponding pixels, reflecting image distortion. Normalized Absolute Error (NAE) measures average pixel-wise deviation, aiding in error analysis and optimization.

TABLE I: Average HVS Parameters

SSIM	PSNR	NCC	MSE	NAE
100%	∞	100%	0	0

Table I presents the average HVS parameters computed from the initial secret medical image and the reconstructed images. The tabulated HVS values show that the algorithm provides maximum reconstruction.

Embedding capacity is calculated using BPP using Eq. 2. Average BPP and PSNR values are tabulated and compared with the state-of-the-art method in Table II. The tabulated values show that the proposed framework achieves better BPP and PSNR than state-of-the-art methods.

$$BPP = \text{Embedded data size in bits} / \text{Total number of pixels in the image} \quad (2)$$

Here, $PSNR^{org(enc)}$ represents the PSNR between the embedded image and the original image, and $PSNR^{org(recon)}$ represents the PSNR between the original and reconstructed image.

TABLE II: Performance comparison of the proposed scheme with similar schemes

Scheme	BPP	$PSNR^{org(enc)}$	$PSNR^{org(recon)}$
Proposed scheme	2.631	27.654	∞
X. Xiong et al [19]	2.250	41.9730	∞
Xiao et al [20]	0.4844	12.1328	∞
Malik et al. [21]	0.4902	-	∞
Bhardwaj and Aggarwal [22]	2.2412	42.0391	∞

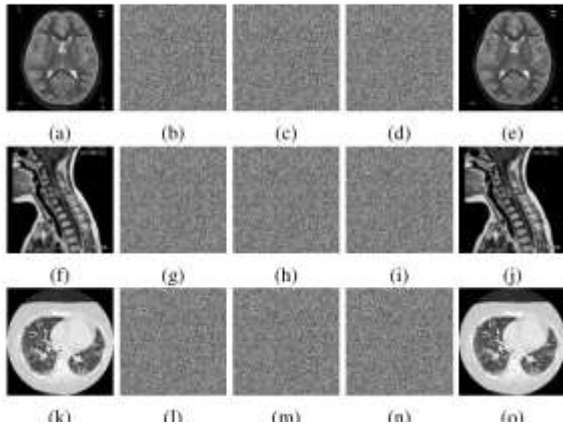


Fig -4: (a) Input image MI1, (b),(c),(d) corresponding RG1, RG2, RG3 for input image MI1, (e) Reconstructed image corresponding to MI1, (f) Input image MI2, (g),(h),(i) corresponding RG1, RG2, RG3 for input image MI2, (j) Reconstructed image corresponding to MI2, (k) Input image MI3, (l),(m),(n) corresponding RG1, RG2, RG3 for input image MI3, (o) Reconstructed image corresponding to MI3.

B. Security analysis

This section evaluates the security level by analyzing the quality of the generated shares. The generated share is compared with the original image using MSE, PSNR, and SSIM and tabulated in Table III. The tabulated values show no similarity between the generated shares and the original image. Thus, the proposed exhibits good shared quality concerning security perspective. Entropy is a metric that evaluates the algorithm's security against different statistical attacks. The ideal entropy is achieved when all symbols in the data (image) have equal probability. The mathematical equation used to calculate entropy is represented in Eq. 3.

TABLE III: Security analysis

	MI Vs RG1	MI Vs RG2	MI Vs RG3
MSE	19031	10007	18375
PSNR	5.33	7.33	5.48
SSIM	0.64%	0.194%	0.72%

TABLE IV: Entropy of encrypted image

Scheme	Proposed Scheme	[19]	[23]	[24]
Entropy	7.69	7.98	7.99	6.87

$$Entropy = - \sum_{i=1}^n P_i \cdot \log_2 P_i \quad (3)$$

where P_i is the probability of the i -th symbol present in the digital data.

The ideal entropy value is eight since the proposed framework generates grayscale shares with 256 symbols. Given that the entropy of each share is nearly eight, it indicates that all the 256 symbols present in the share

have equal probability. This equal probability makes the cryptosystem immune to different types of entropy attacks. From Table IV, it is evident that the proposed framework meets the requirement for the utmost level of security.

V. CONCLUSION

This paper presents an effective VSS mechanism for sharing medical images and associated data. Here, a random grid-based approach is used for share generation, and the PBT method hides the associated text in the image. As the generated shares are stored in a distributed manner, the proposed method completely avoids single-point attacks. The proposed method exhibits good reconstructual quality and security. The algorithm requires all the generated n shares to reconstruct the initial image. This property enhances the algorithm's ability against brute force and other statistical attacks. The main drawback of the system is the inability to reconstruct the original image in the case of share tampering. So, our future work will concentrate on tamper detection and self-recovery of shar

REFERENCES

- [1] Alaa A. Abd-alrazaq, Bridgette M. Bewick, Tracey Farragher, Peter Gardner, "Factors that affect the use of electronic personal health records among patients: A systematic review", International Journal of Medical Informatics, Volume 126, 2019.
- [2] V. Teja, P. Banerjee, N. N. Sharma and R. K. Mittal, "Quantum cryptography: State-of-art, challenges and future perspectives," 2007 7th IEEE Conference on Nanotechnology (IEEE NANO), Hong Kong, China, 2007, pp. 1296-1301, doi:10.1109/NANO.2007.4601420.
- [3] Wu X, Yang C-N, "A combination of color-black-and-white visual cryptography and polynomial based secret image sharing", J Vis Commun Image Represent 2019;61:74-84.
- [4] Cimato S, De Santis A, Ferrara AL, Masucci B, "Ideal contrast visual cryptography schemes with reversing", Inform Process Lett 2005;93(4):199-206.
- [5] Tuyls P, Hollmann H, Lint J, Tolhuizen L, "XOR-based visual cryptography schemes", Des Codes Cryptogr 2005;37(1):169-86.
- [6] Li P, Yang C-N, Kong Q, Ma Y, Liu Z., "Sharing more information in gray visual cryptography scheme", J Vis Commun Image Represent 2013;24(8):1380-93.
- [7] Wu X, Lai Z-R, "Random grid based color visual cryptography scheme for black and white secret images with general access structures", Signal Process, Image Commun 2019;75:100-10.
- [8] V. M. Ajmal Mohammed and P. Samundiswary, "An XOR-based Multiple Medical Image Sharing using Visual Secret Sharing," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 793-799, doi: 10.1109/ICESC57686.2023.10192985.
- [9] M. Naor and A. Shamir, "Visual cryptography," in Workshop on the Theory and Application of Cryptographic Techniques, pp. 1-12, Springer, 1994.
- [10] Chin-Chen Chang, Chia-Chen Lin, T Hoang Ngan Le, Hoai Bac Le, "Self-verifying visual secret sharing using error diffusion and interpolation techniques", IEEE Transactions on Information Forensics and Security 4 (4), 790-801, 2009.
- [11] Ching-Nung Yang, Chi-Sung Lai, "New colored visual secret sharing schemes", Designs, Codes and cryptography 20, 325-336, 2000.

[12] Xiaotian Wu, Wei Sun, "Improving the visual quality of random grid-based visual secret sharing", *Signal Processing* 93 (5), 977-995, 2013.

[13] Tzung-Her Chen, Kai-Hsiang Tsao, "User-friendly random-grid-based visual secret sharing", *IEEE Transactions on Circuits and Systems for Video Technology* 21 (11), 1693-1703, 2011.

[14] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, "Reversible data hiding", *IEEE Transactions on circuits and systems for video technology* 16 (3), 354-362, 2006.

[15] Xinpeng Zhang, "Reversible data hiding in encrypted image", *IEEE signal processing letters* 18 (4), 255-258, 2011.

[16] Yaomin Wang, Gangqiang Xiong, Wenguang He, "High-capacity reversible data hiding in encrypted images based on pixel-value-ordering and histogram shifting", *Expert Systems with Applications* 211, 118600, 2023.

[17] Hsien-Wen Tseng, Chi-Pin Hsieh, "Prediction-based reversible data hiding", *Information Sciences* 179 (14), 2460-2469, 2009.

[18] Yang C-N, Wang D-S, "Property analysis of XOR-based visual cryptography", *IEEE Trans Circuits Syst Video Technol* 2014;24(2):189-97.

[19] Xiangguang Xiong, Siyao Zhong, Yu Lu, Separable and reversible data hiding scheme for medical images using modified Logistic and interpolation, *Biomedical Signal Processing and Control*, Volume 87, Part B, 2024.

[20] D. Xiao, Y. Wang, X. Tao, S. Bai, High-payload completely reversible data hiding in encrypted images by an interpolation technique, *Front. Inf. Technol. Electron. Eng.* 18 (11) (2017) 12, <http://dx.doi.org/10.1631/FITEE.1601067>.

[21] A. Malik, H. Wang, T. Chen, T. Yang, A.N. Khan, H. Wu, Y. Chen, Y. Hu, Reversible data hiding in homomorphically encrypted image using interpolation technique, *J. Inf. Secur. Appl.* 48 (2019) 102374, 10.1016/j.jisa.2019.102374.

[22] R. Bhardwaj, A. Aggarwal, An enhanced separable reversible and secure patient data hiding algorithm for telemedicine applications, *Expert Syst. Appl.* 186 (2021) 115721, <http://dx.doi.org/10.1016/j.eswa.2021.115721>.

[23] Yang, Y.; Chang, R.; Feng, X.; Li, P.; Chen, Y.; Zhang, H. An n-Dimensional Chaotic Map with Application in Reversible Data Hiding for Medical Images. *Entropy* 2024, 26, 254. <https://doi.org/10.3390/e26030254>.

[24] Kiran et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 925 012028 doi:10.1088/1757-899X/925/1/012028.