EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Multimedia Encryption Using Rubik's Cube-Inspired Algorithm: A Novel Approach to Audio and Image Security

Vani H Y[1], Anusuya M A[1], Shwethashree G C[1], KB Drakshayini[2] and Vinod D S[1]*

[1]JSS STU, JSS Technical Institutions campus
[2]ATME College of Engineering, Mysuru

Abstract

This paper presents a fast and secure image and audio encryption scheme based on the principles of a Rubik's Cube. The proposed method combines scrambling and XOR-based diffusion to ensure confidentiality during storage and transmission. Multimedia data are converted into matrix representations and permuted using randomly generated row and column secret keys. Circular shift operations are applied based on the parity of the key values to achieve effective confusion and diffusion. This paper highlights the application of rubric cube algorithm applied on audio data for the first time for encryption and decryption process for voice biometric system design. The experimental results are also presented on par to image data with execution time. Audio data is processed and modelled as a three-dimensional Rubik's Cube and scrambled cube using random rotational transformations. Decryption is performed using inverse operations with identical keys. Experimental results confirm strong security, low computational complexity, and high reconstruction accuracy, demonstrating suitability for secure multimedia communication.

Keywords: Confusion and Diffusion, XOR-Based Encryption, Permutation–Substitution Network, Symmetric Key Cryptography, Image and Audio Encryption, Rubik's Cube Algorithm, Data Transmission, Symmetric Encryption

Received on 18 August 2025, accepted on 10 November 2025, published on 17 March 2026

doi: 10.4108/eetiot.9985

*Corresponding author. Email: dsvinod@jssstuniv.in

1. Introduction

In today's world biometric security has gained the interest of authentication system by leveraging physiological and behavioural characteristics to identity verification. Adoption of biometric authentication drives highest accuracy by enhancing usability and reduction on physical artifact. Apart from these advantages their exist challenges related to privacy preservation, ethical compliance, and data security. Biometric data possess an irrevocable nature. This nature cannot be reissued or reset in the form of passwords or cryptographic keys. This necessitates robust protection mechanisms for biometric templates in the phase of storage and transmissions. There exist two types of biometric applications namely physiological and behavioural [2]. Physiological biometrics are derived through static patterns whereas the dynamic patterns are used for behavioural. Human activities like voice characteristics, gait dynamics and keystroke behaviour are considered for implementation. Among these voice

biometrics has emerged as a prominent and practical solutions for non-invasive acquisition with minimal hardware requirements. Voice recognition is hybrid of physiological properties of the vocal tract and behavioural attributes of speech production system. This provides a rich feature space for biometric discrimination. Voice biometric systems abstract and analyse speech features majorly like pitch, formant frequencies, spectral characteristics and prosodic patterns. These applications determine the identity of an unknown speaker from a predefined population that can be used for biometric and person recognition system.

The integration of voice biometrics with encryption mechanisms significantly enhances authentication security and system resilience. Cyphering ensures voice templates and transmitted audio signals remain unintelligible to adversary's environmental conditions by mitigating the risks such as eavesdropping, spoofing, and replay attacks. Encrypted voice metric also enables multi-factor authentication frameworks by considering key type, size, and cryptographic (ciphering and deciphering) process to achieve higher assurance levels.

In this work, encryption- decryption scheme based on the Rubik's Cube algorithm is proposed to enhance the security of voice biometric authentication systems using audio and image data. The method adopts permutation, circular shifts, XOR operations, Cube shifting and diffusion operations, including bitwise transformations with random key generation to effectively challenge audio data. Inverse transformations are applied to reconstruct the original audio signal with high fidelity in the decryption process. The decrypted voice data samples are subsequently matched against registered biometric templates to accomplish authentication. The main objective of this proposed work is to strengthen the confidentiality and robustness of voice biometric systems with minimum computational burdens for real-time Processing. This is achieved by retaining the principles of confidentiality, integrity and availability of secure communication applications.

2. Literature Survey

This section explains the related work based on Rubik's cube algorithm applied for encryption. The literature available presents the application of rubric algorithm only to image processing. Few of the related works are as stated bellows. The Rubik's Cube has gained its popularity to its intrinsic algorithmic complexity, high permutation capability and for strong diffusion characteristics. It is widely used for securing coloured images, medical imagery, video data, and audio signals. A Survey on these is presented in [5] with a comprehensive explanation. Rubik's Cube–based encryption scheme for colour images of arbitrary dimensions for 128-bit symmetric key is proposed in [6]. This article discusses the algorithm application to enhance confidentiality and resistance against brute-force attacks. Paper [7] depicts its applications for medical image security as a chaotic key-driven encryption algorithm. The authors have demonstrated encryption for diagnostically sensitive regions in turn that reduces computational overhead by maintaining data privacy for real-time healthcare applications. The algorithm is further improved by enhancing the cubic structures and identified as Rubik's Revenge Cube algorithm. Its application is demonstrated [8] to generate complex puzzle permutations by forming a mathematical puzzle group. This paper demonstrates nonlinear substitution boxes (S-boxes) resulting in improved resistance against cryptanalytic attacks. Different Key generation techniques for image processing is also discussed extensively in this paper. Paper [9] discloses about the logistic chaotic maps combined with shift to generate highly random encryption keys by improving key sensitivity and unpredictability for image datasets. Ulti-dimensional security is discussed [10] image encryption. This method is also demonstrated for strong resistance to statistical, differential, and correlation-based attacks by validating its cryptographic robustness. Paper [11] presents 3D Bit-Level Encryption using Rubik's Cube permutations with three-dimensional bit-level scrambling. This approach showed the performance of the diffusion and confusion operations by simultaneously operating in spatial and bit planes. Colour image encryption method utilizing alternate quantum random walks and controlled Rubik's Cube [12] operations across RGB colour channels is applied by offering enhanced randomness and security. Hybrid key space expansion techniques were explored in [13], where pseudo-random number generation and modified thresholding were applied using Sudoku-based structures for varying key sizes. These techniques were discussed for symmetric and asymmetric key keys for diverse image types.

From the above survey it is clearly evident that basic and variations on Rubik's cube algorithm is versatile experimented on the image data but not voice data. Hence this gap of application made us curious and motivated us to apply the basic model of the algorithm on voice data. The performance of the algorithm is verified for various data samples of audio and image data sets by considering various validation metrics for files of various.

Data set:

For the applications 10 Image and 8 audio samples are considered and applied on google data sets of varying file sizes between 2 to 20 MB. Various image files like human face, iris, biometric and animal images are considered and the normal voice sample without disfluencies at the word level comprising small phrases are considered for the simulation purposes. The voice samples are varied from small to medium word phrases. The voice dataset offers

various by covering normal speech acquired in normal environments with different sounds.

3. Methodology

The below section explains the various steps adopted for processing and modelling the data in terms of encryption and decryption process preformed using Rubik cube algorithm. This section also outlines the parameters that influenced that algorithm to yield good solutions for audio dataset.

a) Data preprocessing: Audio samples are quantised and processed for uniform amplitude levels by subjecting to normalization process. Common environmental noises are eliminated by editing the audio samples using Praet software without data loss. These samples are quasi segmented into fixed-length frames to facilitate mapping into encryption structure. Similarly, Image samples are subjected to denoising process, colour space conversion and pixel intensity to reduce redundancy, pixel intensity. This influences on encryption efficiency.

b) Encryption and decryption procedure: The methodology adopted for image and audio data encryption and decryption is as follows:

General steps of Rubik cube algorithm:

Pre-processed Image/audio data is formed to be a matrix to be encrypted.

i. Identify Row and column key vector
ii. Decide maximum number of iterations

Step1: Initialization: Determine the dimensions of the encrypted and decrypted image/audio vectors for specified sequence of rows and columns at each phase.

Step 2: Circular Shifts:

- **Step1:** For each row in the image/audio matrix(vector)- Calculate the sum of the elements in that row using modulo 2 operations.

- **Step2:** If the result is 0-Performing a right circular shift on the row by the corresponding value in the row key vector

Else

- Perform a left circular shift on the row by the corresponding value in the row key vector in the case of encryption

Step 3: XOR Operations: For each element in the audio/image matrix Apply XOR operations with the corresponding elements from the column key vector.
Repeat the above process for both encryption and decryption of audio and image samples.

Step 4: The resulting matrix represents the encrypted/decrypted image or audio data.

Figure 1 and 2 represents the flow chart of image and audio data encryption and decryption process.

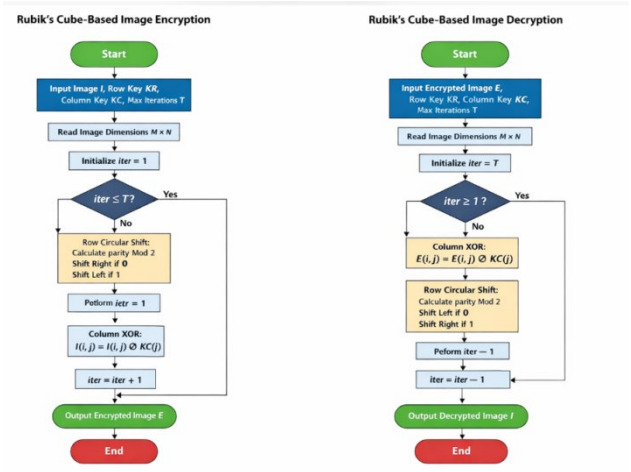

Figure 1. Image data encryption and decryption process

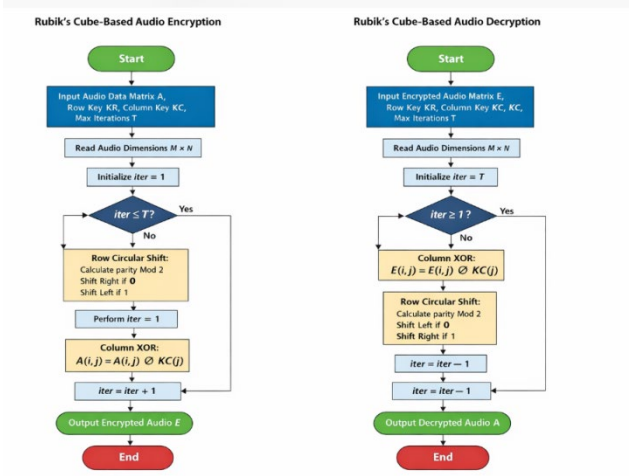

Figure 2. Audio data encryption and decryption process

c) Influential Parameters-Performance: The algorithm leverages cube rotations to generate complex permutations of data blocks ensuring strong confusion and diffusion (no. rounds shifts XOR).

- Different rotation sequences act as encryption keys(public/pry), allowing a vast key space having key flexibility (key size).
- Rotation has a precise inverse used to compute the accurate decryption without data loss hence reversibility is with high data retention.

•The algorithm is highly scalable and can be extended to higher dimensions to handle high-resolution images or long audio streams.

4. Evaluation Metrics

The proposed encryption scheme is evaluated using standard image and audio metrics considering MAE, SSI, histogram uniformity, correlation coefficients, Bit Error Rate, Number of Pixel Change Rate (NPCR), Unified Average changing intensity (UACI) and Peak Signal to Noise Ratio (PSNR). Experimental results are tabulated for the above metrics for the various sizes of audio and image datasets.

1. Mean Absolute Error

The MAE is calculated using the following equation

$$MAE=\frac{1}{x}*\sum t_i-\hat{t_i} \quad \text{Eq. (1)}$$

Where $t_i$is the value observed for observation i

$\hat{t}_i$ is the predicted result for i

$x$is the size considered for experimentation

2. Root Mean Square Error

$$A=\sqrt{\frac{1}{x}\sum(t_i-\hat{t_i})^2} \quad \text{Eq. (2)}$$

Where

x is the size considered for experimentation

$t_i$is the value observed for observation i

$\hat{t}_i$ is the predicted result for i

3. Structural Similarity Index

$$SIM(m,n)=\frac{(2\mu_m\mu_n+d_1)(2\sigma_{mn}+d_2)}{(\mu_m^2+\mu_n^2+d_1)(\sigma_m^2+\sigma_n^2+d_2)} \quad \text{Eq(3)}$$

$\mu_m-Sample\ mean\ for\ pixel\ size\ m$

$\mu_n\ Sample\ mean\ for\ pixel\ size\ m$

$\sigma_m^2\ varaiance\ \ of\ m$

$\sigma_n^2 varaiance\ \ of\ n$

m,n=encryption, decryption values

4. Histogram Correlation

$$d(H_1,H_2)=\frac{\sum_I(H_1(I)-\bar{H_1})(H_2(I)-\bar{H_2})}{\sqrt{\sum_I(H_1(I)-\bar{H_1})^2\sum_I(H_2(I)-\bar{H_2})^2}} \quad \text{Eq(4)}$$

(1) Normalized Cross Correlation

$$\text{norm\_corr}(x,y)=\frac{\sum_{n=0}^{n-1}x[n]*y[n]}{\sqrt{\sum_{n=0}^{n-1}x[n]^2}*\sqrt{\sum_{n=0}^{n-1}y[n]^2}} \quad \text{Eq(5)}$$

5. Peak Signal-to-Noise Ratio (PSNR):

$$PSNR=10Log_{10}\left(\frac{255^2}{MSE}\right) \quad \text{Eq (6)}$$

6. Bit Error Rate (BER)

$$I(X;Y)=\sum_{y\in Y}\sum_{x\in X}p(x,y)\log\left(\frac{p(x,y)}{p(x)p(y)}\right) \quad \text{Eq(7)}$$

Where p(x,y) is the joint probability

Marginal probability is represented by p(x) and(y)

7. Mutual Information (MI): it is the intensity-based similarity measures

$$MI=\sum_i p(i)\log\left(\frac{p(i)}{p(i_A)\,p(i_B)}\right) \quad \text{Eq(8)}$$

8. Number of Changing Pixel Rate (NPCR) $NPCR=\frac{\sum_{i,j}D(i,j)}{WxH}x100\%$ Eq(9)

9. Unified Average Changing Intensity (UACI)

$$UACI=\frac{1}{WxH}\left[\sum_{i,j}\frac{|A(i,j)-B(i,j)|}{255}\right]x100\% \quad \text{Eq (10)}$$

The evaluation metrics are essential for assessing the performance of image and audio processing systems from multiple perspectives. Numerical reconstruction and signal distortion accuracy is calculated using MAE and RMSE metrics. Extended to this metrics PSNR is calculated to observe the perceptual and visual quality along with its structural similarity for auditory fidelity and visual perceptuality. To quantify information leakage and transmission reliability BER metric is applied to realise the difference between encryption and decryption process. To access the sensitivity of the data NPCR and UACI metrics are calculated. All the values are calculated and tabulated decrypted samples v/s original samples to realises the lossy and lossless decryption process. Together, these metrics ensure a rigorous, multidimensional performance assessment.

5. Simulation Results

The Performance results are discussed and observed at three phases of our experimentation on varying file size of audio and image datasets as listed below:

i) Evaluation metrics

ii) Histogram representation

iii) Execution time

i) Evaluation metrics: Different evaluation metrics are considered for audio and image data to identify the accuracy and the performance of the algorithm. Below table 1 presents the various metric values for the encryption and decryption process of an image that consists of various types of image audio datasets. Few considered images are depicted from figure 2a-2d.

Audio samples: Since audio samples are 1Dimensional data, only major and required metrics are used to validate and verify the encrypted and decrypted samples, namely MAE,RMSE and PSNR.

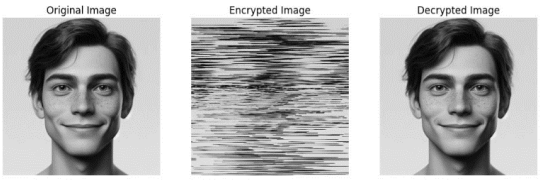

Figure 2a

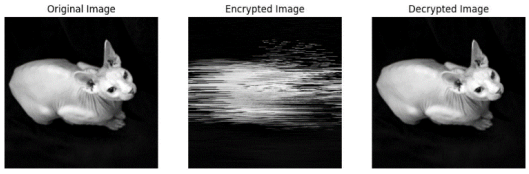

Figure 2b

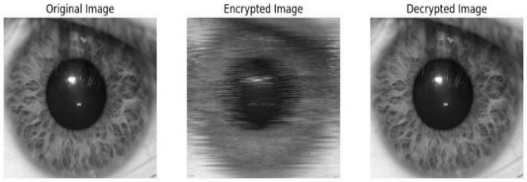

Figure 2c

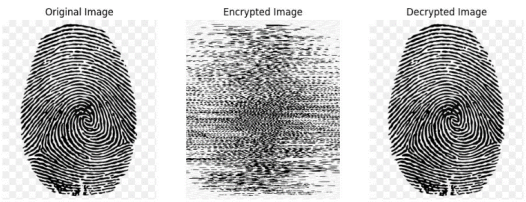

Figure 2d

Figure 2a-2d Original, encrypted and decrypted images

Below table 1a and1b tabulates the values for various metrics.

Table 1a and Table 1b

Table 1: Evaluation Metrics -For Image Data

FILE	MAE	RMSE	SSIM	HC	NCC	PSNR	BER	NPCR(%)	UACI
1	106.34	8.75	0.0598	0.9999	0.1914	29.29	0.39	99.63	33.69
2	91.41	6.77	0.420	1.0	0.718	31.51	0.25	99.61	33.41
3	88.63	5.74	0.0422	1.0	0.177	32.95	0.37	99.60	33.48
4	123.32	9.17	0.20	1.0	0.796	28.87	0.41	99.61	33.67
5	124.32	9.18	0.21	1.0	0.798	28.89	0.41	99.59	33.62
6	107.34	8.75	0.0598	0.9999	0.1914	29.29	0.39	99.49	33.65
7	90.41	6.77	0.420	1.0	0.718	31.51	0.25	99.45	33.61
8	86.63	5.74	0.0422	1.0	0.177	32.95	0.37	99.43	33.62
9	108.34	8.75	0.0598	0.9999	0.1914	29.29	0.39	99.47	33.45
10	89.63	5.74	0.0422	1.0	0.177	32.95	0.37	99.45	33.65

Table 1b Evaluation Metrics for Audio Data

FILE	MAE	PSNR	BER	NPCR (%)
1	108.64	32.57	0.49	99.63
2	87.41	28.89	0.15	99.51
3	98.63	32.95	0.47	99.40
4	108.32	29.87	0.47	99.71
5	134.32	27.89	0.48	99.59
6	109.34	25.29	0.49	99.39
7	89.41	35.51	0.25	99.43
8	76.63	36.95	0.27	99.23
9	109.34	28.29	0.39	99.87
10	89.63	32.95	0.37	99.45

The metric values are compared with the original image and the decrypted image. The difference values are tabulated in table 1a. From the table it is evident that the NPCR metric values are all approximately near to 98%. This demonstrates the algorithm retains the quality of the image data even after decryption. It is also observed that rubric cube performs equally good for audio data also. The BER value in the table is small varying from 0.2 to 0.3. Hence the algorithm has greater flexibility in performances and applications. Hence it can be recommended to apply to the applications of voice metrics and security domains to utilise its benefits due to its reduced bit error rate (BER).

ii)Results using histogram representation: For image samples (Figure 2a-2d), the histogram areplotted for image and audio files. Image file reflects the distribution of pixel intensities across grayscale levels (0–255) or across individual RGB channels. Rubik cube algorithm significantly alters the distribution, producing a nearly uniform histogram for the cipher image represented through spikes. This uniformity indicates reduced statistical redundancy and resistance against statistical attacks. After decryption, the histogram of the recovered image is closely matched with that of the original image, demonstrating lossless or high-fidelity reconstruction. Figure 3a – 3h represents the histograms of encrypted and decrypted images of figure 2a-2d.

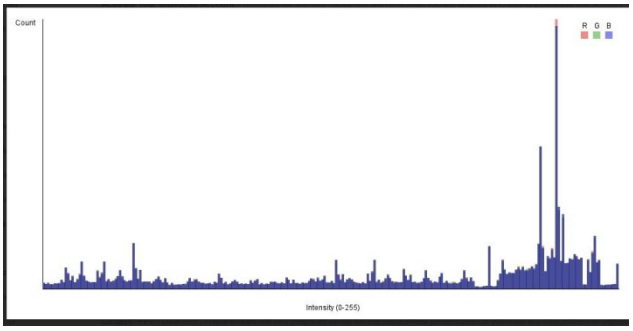

Figure 3a. Human face-encryption

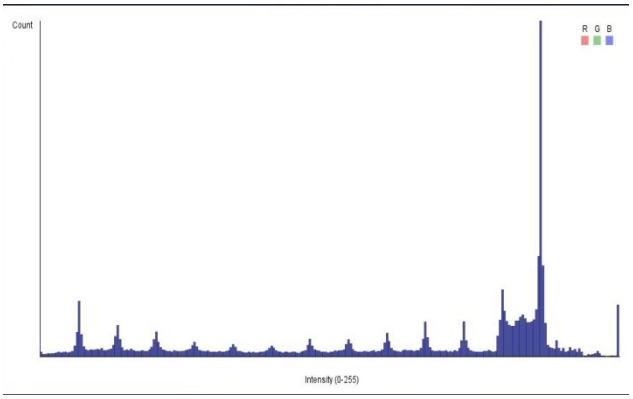

Figure 3b. Human face-decryption

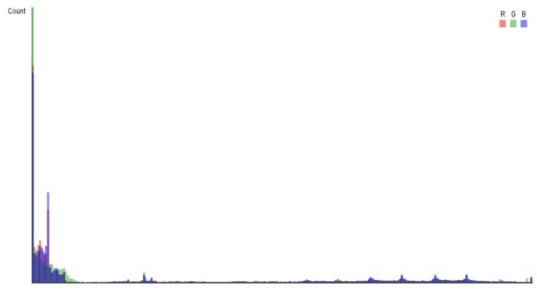

Figure 3c. Rabbit image encryption

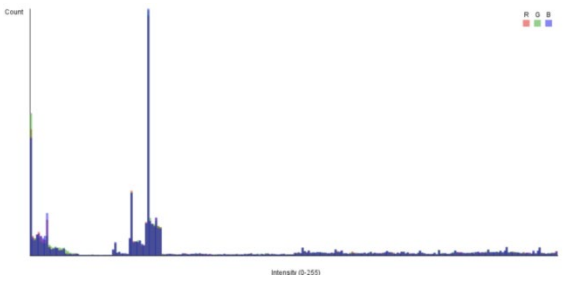

Figure 3d. Rabbit image decryption

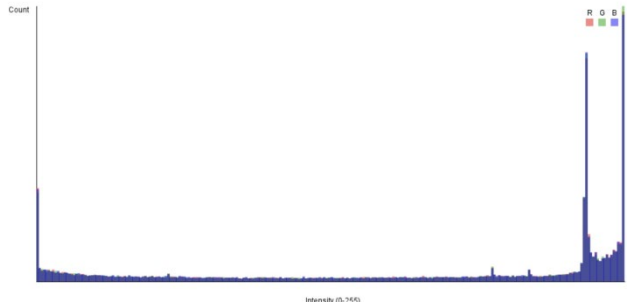

Figure 3e. Biometric image encryption

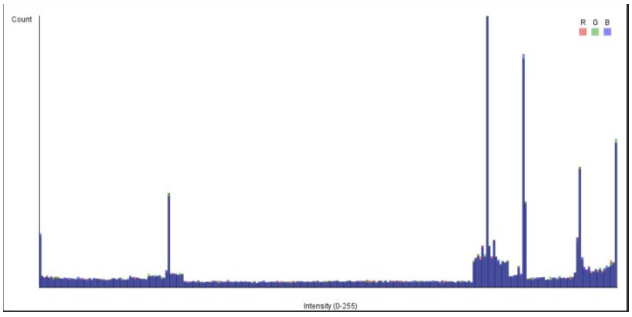

Figure 3f. Biometric image decryption

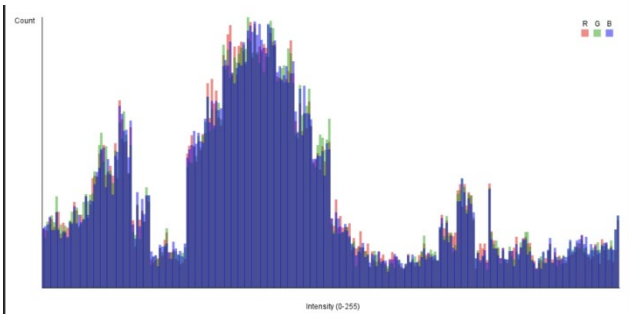

Figure 3g. Eye image encryption

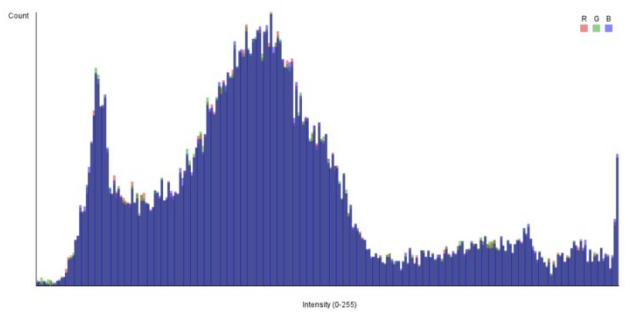

Figure 3h. Biometric image decryption

Figure 3a-figure 3h presents the histogram plots for the images 2a-2d at encryption and decryption levels.

Similarly, for audio samples, the histogram represents the distribution of signal amplitude values. The histogram of audio signal is processed for audio signal quality, amplitude distributions exhibiting structured patterns depending on speech characteristics. Cube shifts of the algorithm highlight the encryption method by disrupting the patterns, yielding a flattened or randomized distribution in the encrypted audio signal. In the process of decryption, the histogram reverts to a distribution nearly identical to the original signal, confirming accurate signal recovery.

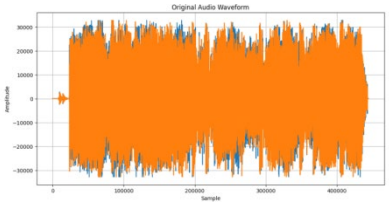

Figure 4a. Original Audio waveform

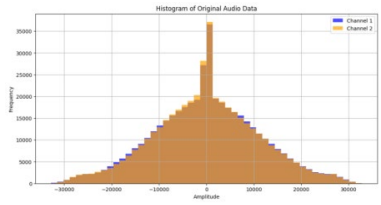

Fig 4b. Histogram of Original Audio waveform

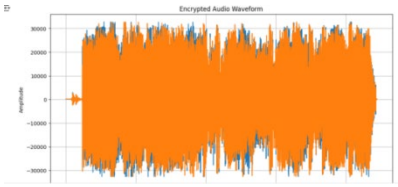

Fig 4c. Encrypted Audio waveform

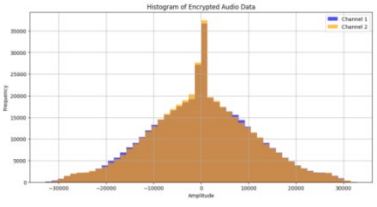

Figure 4d. Histogram of Encrypted Audio waveform

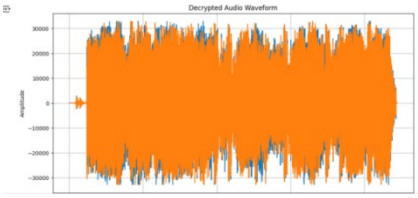

Figure 4e. Decrypted Audio waveform

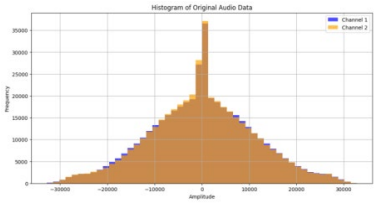

Figure 4f. Histogram of Decrypted Audio waveform

The audio files are processed together in a pool as depicted from figure 4a-4f. These represents the original, encrypted and decrypted audio files. Since the skewness and the uniform width of the histograms are equal, the decryption process using rubric cube can be proposed as one of the ciphering techniques for security domains.

iii) Results using execution time:

This section explains the algorithmic performance in terms of time computation for an encryption and decryption of audio and image samples. Table 2 documents execution times and energy used in running the rubric cube algorithm for audio samples. Since audio samples are nonstationary and nonlinear in nature it is very difficult to parameterise crucially. The figure 4a-4f depicts the original, encrypted and decrypted waveforms histogram along with the corner values of the cube when seeded with 12353 values in the process of decryption. The rotation values of the cube for one layer are as shown in the figure 5 for the decryption process. Figure 6 plot the performance analysis of encryption and decryption process time taken by the algorithm. It is observed that decryption process takes lesser time even in the increase in the size of data. This feature promotes the applicability of the algorithm even for large file sizes of multimedia and multimodal datasets.

Cube after reverse scrambling corners with seed 12353

Current Cube State:
Layer0:
[53,56,59,10]
[7,48,60,50]
[47,51,63,4]
[54,50,62,63]
Layer3:
[48,32,8,60]
[59,54,58,56]
[55,53,57,52]
[0,55,52,58]
Cube after reverse rotating layer 0:

Layer3:
[48,32,8,60]
[59,54,58,56]
[55,53,57,52]
[0,55,52,58]

Cube after reverse rotating face2:

Layer3:

[48,32,8,60]
[59,54,58,56]
[55,53,57,52]
[0,55,52,58]

Cube after reverse XOR on layer 3:

Layer3:

Table 2: Time for Enciphering and Deciphering of Audio Data

Data capacity	Pattern	Cipher Duration(ms)	Decipher Duration(ms)
2MB	Audio	500	500
3MB	Audio	600	600
5 MB	Audio	2000	1800
10 MB	Audio	4000	3800
15 MB	Audio	6000	5800
20 MB	Audio	8000	7800

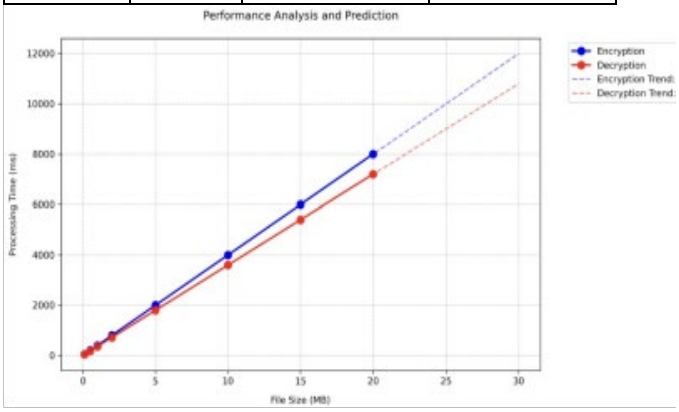

Figure 6. Performance Analysis of encryption and decryption

Over all observations:

The execution results show that encryption and decryption times increase as image/audio data capacity grows from 2 MB to 20 MB. For larger files (10–20 MB), the increase in processing time is nearly proportional to the input size, indicating approximately linear time complexity. From this it is proved that the scaling of the algorithm can be extended for larger image and audio samples. It is observed

[3,1,13,5]
[49,3,0, 37]
[25,15,12,21]
[57,2,14,53]

Cube after reverse scrambling corners with seed12349:

Layer3:
[48,1,13,6]
[31,3,0, 37]
[22,15,12,21]
[5,11,8, 15]
Final output data after decryption:

[53,1,2,9,4,5,6,7,8,9,10,11,0,13,14,15,16,17,18,19,20,21
,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,
40,41,42,43,44,45,46,47,60,49,50,63,52,53,54,55,56,57,
58,59,3,61,62,51]

that if the variations in the sample size are small the execution times demonstrating operational symmetry. This feels the algorithm performance is identical. But if the file size is moderate or high decryption is slightly faster than encryption with minimal execution time. This results in balancing computationally consistency in forward and inverse Rubik's Cube transformations. The growth remains stable and predictable even the execution time increases for larger file samples. Generally, for the data samples the algorithm validates scalable performance and balanced processing overhead for audio communication biometric and communication systems.

6. Conclusions & Future enhancement

This work highlights the Rubik's Cube algorithm offers systematic framework for audio data processing as similar to image by retaining the audio and image data it also equally performs well for audio data sample maintaining perceptual quality in terms of precision, less execution time in terms of decryption and efficiency irrespective of the samples size. The paper also contributes towards the application of the Rubik cube algorithm applicability for the audio samples for the first time in the field of voice biometric applications. Algorithms layering approach helps to manipulate and optimize the complex multimedia inputs and outputs for increasing the strength of the algorithm for various levels of authentication like one or two step authentications. Its structured nature allows for adaptability, flexibility and scalability in the network by strengthening the algorithm when applied to voice biometric applications. This approach not only maximizes quality but also enhances the algorithm's versatility for all domains. With consistent application and customization, the Rubik's Cube algorithm becomes a reliable tool for achieving superior outcomes in multimedia applications. Further the algorithm can be enhanced by hybrid Ing AES algorithm to strengthen the security concepts. Further the application can be applied and verified for dynamic key mechanism with multilevel encryption framework. This algorithm is planned to apply the stuttering speech samples

to note the differences between the various disfluencies of speech patterns.

References:

[1] Mane, J.S., Bhosale, S. (2023). Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. Revue d'Intelligence Artificielle, Vol. 37, No. 3, pp. 709-718. https://doi.org/10.18280/ria.370319

[2] Shaveta Dargan, Munish Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, Expert Systems with Applications, Volume 143,2020,113114, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2019.113114.

[3] Review on Encryption of Video: Determination Optimal Measures for Robust Video Encryption AtaaRasol Alawi NidaaFlaih Hassan Department of Computer Science, University of Technology, Baghdad, Iraq

[4] N. K. Ratha, J. H. Connell and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," in IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001, doi: 10.1147/sj.403.0614.

[5] Demaine, Erik D. et al. "Algorithms for Solving Rubik's Cubes." Algorithms – ESA 2011.
Ed. Camil Demetrescu & Magnús M. Halldórsson. LNCS Vol. 6942. Berlin, Heidelberg: Springer
Berlin Heidelberg, 2011. 689–700.

[6] Aditi Nair, DitiDalal, Ramchandra Mangrulkar, Colour image encryption algorithm using Rubik's cube scrambling with bitmap shuffling and frame rotation, Cyber Security and Applications, Volume 2,2024, 100030, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100030

[7] R. Vidhya, M. Brindha,A chaos based image encryption algorithm using Rubik's cube and prime factorization process (CIERPF),Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 5,2022, Pages 2000-2016 ,ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2019.12.014.

[8] Yousaf, A., Razaq, A. &Baig, H. A lightweight image encryption algorithm based on patterns in Rubik's revenge cube. Multimed Tools Appl 81, 28987–28998 (2022). https://doi.org/10.1007/s11042-022-11898-0

[9] Sinha, R.K., Agrawal, I., Jain, K., Gupta, A., Sahu, S.S. (2020). Image Encryption Using Modified Rubik's Cube Algorithm. In: Sahana, S., Bhattacharjee, V. (eds) Advances in Computational Intelligence. Advances in Intelligent Systems and Computing, vol 988. Springer, Singapore. https://doi.org/10.1007/978-981-13-8222-2_6

[10] Aditi Nair, Diti Dalal, Ramchandra Mangrulkar, Colour image encryption algorithm using Rubik's cube scrambling with bitmap shuffling and frame rotation, Cyber Security and Applications, Volume 2,2024,100030, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100030.

[11] Hegui Zhu, Lewen Dai, Yating Liu, Lijun Wu, A three-dimensional bit-level image encryption algorithm with Rubik's cube method, Mathematics and Computers in Simulation, Volume 185,2021, Pages 754-770, ISSN 0378-4754, https://doi.org/10.1016/j.matcom.2021.02.009.

[12] Zhao J, Zhang T, Jiang J, Fang T, Ma H. Color image encryption scheme based on alternate quantum walk and controlled Rubik's Cube. Sci Rep. 2022 Aug 22;12(1):14253. doi: 10.1038/s41598-022-18079-x. PMID: 35995941; PMCID: PMC9395402.

[13] Deshpande, K., Girkar, J., & Mangrulkar, R. (2023). Security enhancement and analysis of images using a novel Sudoku-based encryption algorithm. Journal of Information and Telecommunication, 7(3), 270–303. https://doi.org/10.1080/24751839.2023.2183802

[14] Song, Wei & Fu, Chong & Zheng, Yu & Tie, Ming & Liu, Jun & Chen, Junxin, 2023. "A parallel image encryption algorithm using intra bitplane scrambling," Mathematics and Computers in Simulation (MATCOM), Elsevier, vol. 204(C), pages 71-88.

[15] Murari T., V., K C, R. & M E, R. Selective encryption of video frames using the one-time random key algorithm and permutation techniques for secure transmission over the content delivery network. Multimed Tools Appl 83, 82303–82342 (2024). https://doi.org/10.1007/s11042-024-18613-1

[16] Mai Helmy, Walid El-Shafai, El-Sayed M. El-Rabaie, Ibrahim M. El-Dokany, Fathi E. Abd El-Samie,A hybrid encryption framework based on Rubik's cube for cancellable biometric cyber security applications, Optik, Volume 258,2022, 168773, ISSN 003026, https://doi.org/10.1016/j.ijleo.2022.168773.

[17] Suo Gao, Jiafeng Liu, Herbert Ho-ChingIu, UğurErkan, Shuang Zhou, Rui Wu, Xianglong Tang, Development of a video encryption algorithm for critical areas using 2D extended Schaffer function map and neural networks, Applied Mathematical Modelling, Volume 134,2024,Pages 520-537, ISSN 0307-904X, https://doi.org/10.1016/j.apm.2024.06.016.

[18] Rupesh Kumar Sinha and SitanshuSekharSahu, Multi-level image security using modified Rubik's cube algorithm ,International Journal of Information and Computer Security Vol. 23, No. 4

[19] R. Zhao, Y. Zhang, J. Ji, S. Yi, W. Wen and R. Lan, "AES-AUDIO: An Encryption Scheme for Audio Supporting Differentiated Decryption," in IEEE Transactions on Multimedia, doi: 10.1109/TMM.2024.3521757.

[20] Cao, Y., Liu, H. An audio encryption algorithm based on a non-degenerate 2D integer domain hyper chaotic map over GF(2n). Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-18746-3

[21] Zhou, L., Li, X., Tan, F. et al. A two-layer networks-based audio encryption/decryption scheme via fixed-time cluster synchronization. Soft Compute 26, 9761–9774 (2022). https://doi.org/10.1007/s00500-022-07335-x

[22] Parekh, A., Antani, M., Suvarna, K. et al. Multilayer symmetric and asymmetric technique for audiovisual cryptography. Multimed Tools Appl 83, 31465–31503 (2024). https://doi.org/10.1007/s11042-023-16401-x

[23] J. Joy and L. Koshy, "Rubi Crypt: Image Scrambling Encryption System Based on Rubik's Cube Configuration," 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019, pp. 1-8, doi: 10.1109/ICSCAN.2019.8878785.

[24] Khaled Loukhaoukha, Jean-Yves Chouinard, Abdellah BerdaiA Secure Image Encryption Algorithm Based on Rubik′s Cube Principle, Journal of electrical and computer engineering,2012