Ain Shams Engineering Journal 16 (2025) 103193

Contents lists available at ScienceDirect

Ain Shams Engineering Journal

journal homepage: https://www.sciencedirect.com

Full Length Article

A digital audio data protection method using parametric action of generalised triangle group on $GF(2^8)$

Aqsa Zafar Abbasi [a], Ayesha Rafiq [a], Badr M. Alshammari [b,*]

[a] Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, 44000, Pakistan
[b] Department of Electrical Engineering, College of Engineering, University of Ha'il, Ha'il, 81451, Saudi Arabia

ARTICLE INFO

Keywords:
Algebraic structure based S-Box
Audio encryption
Block cipher
Generalised triangle group

ABSTRACT

The parametrization of the action of the modular group $PSL(2,\mathbb{Z})$ for the triangle groups is extended for $\Delta(2,3,k)$ to the finite generalised triangle groups $\langle u,v \mid u^2 = v^3 = w^k = 1\rangle$ where $w = uvuvuv^2uvuv^2$. Also, based on the resulting parametric equations, the authors have presented an audio encryption approach in this study. The extremely secure S-Box, which is then utilised to encrypt audio signals, is built using parametric equations. Utilising several audio sources, the effectiveness of the current approach is assessed. According to the simulation specially differential analysis average NSCR 99.96% and average UACI 33.33% as well as comparison results, the recommended method might prevent cryptographic vulnerabilities and produce reliable encryption results.

1. Introduction

Digital media has become more important in social life in the past few years as a result of the rapid advancements in science as well as digital technology. Numerous fields, including education, math, engineering, military services, medical, research in science, and numerous more employ multimedia information. The need for digital files and tools for analysing multimedia information has increased due to the uncontrollably high growth of multimedia information. The safety and confidentiality of the visual information are at risk due to the unsuitable opportunities that have been generated by this internet-based utilisation of it. Multimedia security of data becomes a hot topic as a result of these dangers. To safeguard private data across public networks, a significant amount of techniques have been developed. Cybersecurity is the most widely used field for assurances, and it is further subdivided into symmetric as well as asymmetric key generation techniques. Many digital audio encryption techniques are reported in the literature. In 2002, Servetti & De Martin [21] developed a method of encryption based on the perception-based approach for telecommunication speech protection. Two methods were suggested by the author for encrypting fragmentary conversation. The author of Thorwirth et al. [25] primarily focused on analysing the data encryption within the encrypted MP3 files while providing a method for the selectively encrypted approach of perceptive audio coding utilising standard reduction. [23] proposed a new audio encryption technique based on permutation networks and replacement. Strong S-Boxes for the substitution network and the Hénon chaotic map, which conducts pixel-wise permutation as utilised for the permutation network, are produced in this study using the Mobius transformation as a source. In [22], the author divided the sound data into two sections, such as eight bits and seven bits. Additionally, they used permutation and substitution techniques to encrypt the data. However, when they decrypted the data, they found that some of the integers in the designated 16-bit range were missing. To facilitate secure cloud processing and communication, a new encryption method for homomorphic audio signals has been developed [12]. In [4], a dual-channel, one-time, one-key audio encoding system built around chaos was suggested.
G. Baumslag et al. in [3] explored generalised triangle groups (GTGs), extending the theory of triangle groups. In 1995 M. Hagelberg et al. investigated discrete generalised triangle groups [10]. G. Rosenberger discussed free subgroups within certain generalised triangle groups [17]. In [3] and [8] it was demonstrated that if $G = \langle u, v : u^r, v^s, \omega^k\rangle$, then the homomorphism $\xi : G \rightarrow PSL(2,\mathbb{C})$ exists such that $\xi(u)$, $\xi(v)$ and $\xi(\omega)$ have orders r, s and k. In 2000, Vinberg et al. clarified pseudo-finite groups of generalised triangles [26]. J. Howie et al. [11] almost completed the classification of finite GTGs and specified the conditions under which these groups remain finite. For details of Galois field and GTG refer to [1]. Q. Mushtaq parametrized all homomorphisms from $PGL(2,\mathbb{Z})$ to $PGL(2,q)$ [18], theory extended by M. Ashiq et al. in

* Corresponding author.
E-mail addresses: zafariqbalabbasi67@gmail.com (A.Z. Abbasi), ayesha_rafiq@live.com, ayesha.rafiq@mail.ist.edu.pk (A. Rafiq), bms.alshammari@uoh.edu.sa (B.M. Alshammari).

https://doi.org/10.1016/j.asej.2024.103193
Received 24 August 2024; Received in revised form 25 October 2024; Accepted 17 November 2024

Available online 4 December 2024

2018 focusing on the non-transitive action $\Delta(2,4,k)$ on $PL(F_q)$ [2]. Recently, in 2020, T. Imran investigated the action of $\Delta(3,n,k)$ on the projective line [16].
In this work, authors developed a new digital audio data protection system based on binary Galois filed $GF(2^n)$ and groups over a finite field $\mathbb{Z}_p$. This scheme's main goal is to offer a robust algorithm that make the encryption stronger. Since the group actions are operating effectively, a special kind of group based on the generalised triangle group is introduced in the suggested scheme. The parametrisation of H_5 for the generalised triangle group $\langle u^2 = v^2 = (uvuvuv^2uv^2)^k \rangle$ has not yet been tied to the substitution box in this scenario in any published research. The $\triangle(2,3,k)$, the homomorphic image of $PGL(2,\mathbb{Z})$ for k to the power of $uvuvuv^2uv^2$, is the major focus of our study.
Comparing the building of an S-Box based on parametric equations of generalised triangle groups to the traditional algebraic structures commonly employed in cryptography designs reveals numerous clear benefits. The rich algebraic and symmetric structure of generalised triangle groups i.e., $u^{\alpha_1}v^{\beta_1}u^{\alpha_2}v^{\beta_2}...u^{\alpha_\xi}v^{\beta_\eta}$ may be used to generate extremely nonlinear and bijective mappings that are necessary for reliable cryptographic functions like diffusion and confusion. In contrast to traditional algebraic techniques for example based on triangle group structures i.e., uv, such those based on finite fields, the parametric equations of generalised triangle groups permit more nonlinearity in the building of S boxes because of its complex structure. Because of its adaptability, a variety of S. Box variations may be created by changing its parameters, offering a greater range of design choices that can be customized to meet certain security needs.
The following highlights the article's key contributions:

1. The parametric action for the GTG is completed by utilising the outcomes of the parametrization of modular group homomorphisms. The formula is $G =< u^2 = v^3 = t^2 = (ut)^2 = (vt)^2 = (uvuvuv^2uv^2)^k >$.
2. To provide a new approach to S-Box creation that makes use of the parametric action of the GTG on $PL(F_{256})$.
3. To evaluate the encryption algorithm's dependability using benchmark tests made specifically for audio encryption techniques.
4. The results will demonstrate how effectively the suggested encryption technique encrypts digital signals.

The remaining article is organised in this manner. Section 2 displays the parametrisation of the modular group action for generalised triangle group $\langle x, y \,|\, x^2 = y^3 = w^k = 1\rangle$ where $w = uvuvuv^2uvuv^2$. In Section 2 also contains the S-Box design strategy based on generalised triangle groups. Section 3 offers a detailed analysis of the proposed S-Box, including its cryptographic properties. In Section 4, the S-Box integration into an audio encryption scheme is described whereas Section 5 is based on experimental results. Section 6, which also offers suggestions for additional study and a synopsis of the findings, serves as the article's conclusion.

2. Parametrization of G.T.G and construction of substitution box

In the past few years, group actions as well as their applications to different mathematical frameworks have attracted a lot of interest. [24] uses a matrix of adjacency constructed on the $GF(2^8)$ to provide a novel method for building reliably encoded 8×8 S-Boxes. Parallel to this, [19] presents a novel construction method for the nonlinear portion of the block cipher, which based on the action of $PGL(2,\mathbb{Z})$ across the $PL(F_q)$ as well as permutation triangle groups. The finite generalised triangle groups $\langle u, v \mid u^2 = v^3 = w(u,v)^k = 1\rangle$ are obtained from this parametrisation, where $k \in \mathbb{Z}^+$ and $w(u,v) = uvuvuv^2uvuv^2$.
Our main goal is to investigate the potential that the activity of generalised triangle groups presents for creating a reliable substitution box. The coset diagram depicting the action can be constructed more easily with the help of the matrices U and V, which correlate to the transformations $\bar{u}$ and $\bar{v}$, respectively. These matrices can be found in the equations that follow which are discussed in [18].

$$\det(U) = -a^2 - kc^2 = \Delta \neq 0, \tag{2.1}$$

$$\det(V) = d^2 + d + kf^2 + 1 = 0. \tag{2.2}$$

$$r = 2ad + a + 2kcf. \tag{2.3}$$

$$s = 2af - 2cd - c. \tag{2.4}$$

$$r^2 + ks^2 = 3\Delta. \tag{2.5}$$

Also,

$$U^2 + \Delta I = 0 \tag{2.6}$$

$$V^2 + V + I = 0 \tag{2.7}$$

$$(UV)^2 + r(UV) + \Delta I = 0 \tag{2.8}$$

For $W = UVUVUVVUVUVV$, using equations (2.6) to (2.8) we get,

$$W = (r^5 - 2r^3\Delta)I + (\Delta^2)U + (r^3\Delta - r\Delta^2)V + (2r^2\Delta - r^4)(UV)$$

Applying trace we get,

$$tr(W) = r(r^4 - 2r^2\Delta + \Delta^2) \tag{2.9}$$

where $tr(U) = 0,\ tr(V) = -1$ and $tr(UV) = r$, with

$$\theta = \frac{(tr(W))^2}{det(W)} \tag{2.10}$$

where $U = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix}$ and $V = \begin{bmatrix} d & kf \\ f & -d-1 \end{bmatrix}$ are the matrix representation of $\bar{u}$ and $\bar{v}$.

2.1. Construction of S-Box

A fundamental aspect of cryptographic algorithms, especially block codes, is the substitution box or S-Box. Adds non-linearity to the encoding process by performing substitution procedures. S-Box is mostly used to hide the connection between encoded and plaintext, making it difficult for attackers to discover the message that was sent from the encoded one. Our primary goal is to build an S-Box for $< u^2 = v^3 = t^2 = (ut)^2 = (vt)^2 = (uvuvuv^2uvuv^2)^k = 1 >$ using the parametric equations of $PGL(2,\mathbb{Z}$ on $PL(F_q)$. By examining every facet of the spare box design, our goal is to increase its effectiveness and safety. Thanks to the illumination provided by this examination of optimisation options and encryption strength, authors will be able to construct S-Boxes that are resistant to a variety of threats and that use efficient interior encryption strategies. To make S-Boxes dependable and useful for real-world applications, the authors work to strike a balance between stringent safety regulations and operating performance. The GTG was employed in medical image encryption using parametric action in [1]
The action of $PGL(2,\mathbb{Z})$ will be examined on $PL\left(F_{2^8}\right)$ in the case of $\theta = 4$ for $w(u,v) = uvuvuv^2uvuv^2$. Using the parametric equations (2.10), (2.1), (2.2), (2.3), (2.4), (2.5) and (2.9), we obtain $a = 31$, $c = 13$, $k = 194$, $d = 211$ and $f = 2$ over characteristic polynomial $\kappa(\phi) = \phi^8 + \phi^4 + \phi^3 + \phi^2 + 1$, then U and V becomes

$$U = \begin{bmatrix} 31 & 218 \\ 13 & 225 \end{bmatrix} \quad V = \begin{bmatrix} 211 & 132 \\ 2 & 44 \end{bmatrix}$$

with linear fractional transformations

$$\bar{u} \to \frac{31z+218}{13z+225} \qquad \bar{v} \to \frac{211z+132}{2z+144}$$

Using the above transformation and performing group action, it becomes

$$(z)(\bar{u}\bar{v}\bar{u}\bar{v}\bar{u}\bar{v}^2\bar{u}\bar{v}\bar{u}\bar{v}^2) = \frac{27z+116}{245z+76} \tag{2.11}$$

Table 1
Proposed S-Box.

	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111
0	65	140	168	224	63	151	141	144	58	165	172	198	236	158	80	199
1	39	206	241	211	138	20	237	202	83	111	207	45	190	46	254	228
10	30	225	9	142	220	153	163	87	53	12	182	132	102	185	214	79
11	117	118	205	169	249	253	184	101	229	175	75	92	227	232	131	192
100	174	110	35	98	216	90	50	95	4	121	196	223	238	16	167	137
101	84	212	54	19	114	188	74	251	21	112	240	193	178	203	248	55
110	78	10	245	100	26	247	37	5	49	86	152	215	255	129	66	41
111	88	204	72	159	33	81	217	29	230	116	32	189	209	24	243	244
1000	166	124	171	2	195	123	139	194	76	119	61	187	109	56	115	18
1001	177	77	44	67	222	91	145	197	51	47	34	3	179	235	73	126
1010	57	234	252	135	155	213	162	15	183	103	130	59	8	181	201	31
1011	156	97	28	242	17	7	69	68	164	200	128	108	146	221	122	99
1100	180	106	27	154	160	173	43	218	250	89	127	82	13	246	40	120
1101	104	176	136	134	36	226	38	148	14	52	60	157	239	107	96	233
1110	125	161	191	70	6	25	231	170	150	48	143	23	210	93	64	133
1111	113	105	11	1	22	71	186	149	147	0	94	208	42	85	219	62

S-Box is constructed by utilizing the derived transformation illustrated in equation (2.11) is presented in Table 1.

3. Analysis of substitution box

Since the “Advanced Encryption Standard (AES)”is the most recent block cipher algorithm standard, 16×16 S-Box configurations have been created in the study in order to increase the accurate assessment and practical utility of the acquired outputs. The primary reason for the 16×16 size of the AES S-Box framework is that it can be quickly implemented in software as criteria for selection in the competition grasped during the development of the standard. Since today’s languages of programming have a byte-based structure, 8 bits in a byte value, the AES S-Box configuration is built as a nonlinear function that transforms 8-bit input to 8-bit output; consequently, the AES S-Box configuration incorporates $2^8 = 256$ elements. A kind of displacement table resembling the AES S-Box structure can be constructed up to 256!. Naturally, it is not possible to employ every possible arrangement of randomly arranged integers in a 16×16 table to create an S-Box structure. Within such combinations, a few cryptological constraints must be satisfied. This section provides a brief explanation of the following criteria/requirements.

3.1. Nonlinearity

An 8-bit input to 8-bit output relationship is provided by the 16×16 S-Box. The accompanying sbox is securely weak if this relationship is linear, which opens the door for attackers to successfully penetrate the ciphertext. More cryptographic protection against attacks is provided by an S-Box if this relationship is thoughtfully made to be non-linear. Those S-Boxes offer a robust defence against linear cryptanalytic attacks in systems built using them. One can compute the nonlinearity value displayed by a n × n S-Box by utilising equation below [5].

$$NL(B) = \frac{1}{2}\left(2^n - W_{max}(B)\right)$$

In this case, B stands for an n-bit boolean function. The value of the “Walsh-Hadamard transformation”is indicated by $W_{max}(B)$. The average S-Box nonlinearity value in this investigation was 112.

3.2. Strict avalanche criteria

Webster and Tavares suggested using SAC to build a powerful S-Box [27]. If any of the input bits are altered, half of the output bits should also change, based on the SAC value. As such, it is deemed sufficient if the SAC value is about equivalent to 0.5. In other words, attackers can gain information if a single bit change in the input impacts a large or small number of bits in the output. For this reason, SAC is a crucial statistic. It is clear by examining the average of these numbers that S-Box is extremely near to 0.5. Stated otherwise, the suggested methodology satisfies the conditions of this standard.

Table 2
Comparison of S-Box’s Performance.

S-Box	NL	S.A.C	BIC-SAC
Proposed Scheme	112	0.5234	0.4998
Scheme 2 [6]	112	0.5010	0.4973
Scheme 3 [14]	106.87	0.509	-
Scheme 4 [20]	110.75	0.5012	-
Scheme 5 [13]	112	0.503	0.5015
Scheme 6 [15]	111.50	0.4878	-

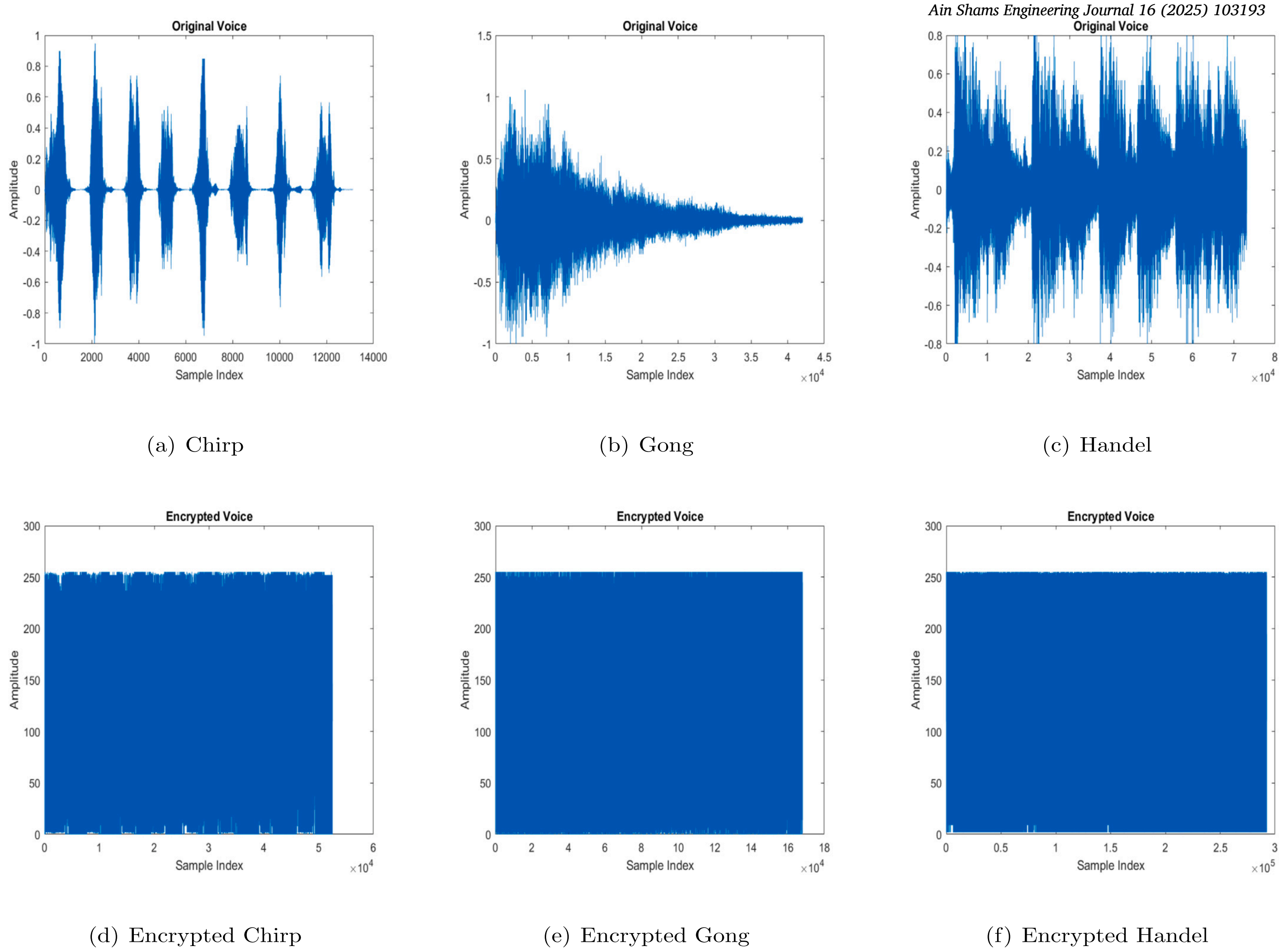
3.3. Bit independent criteria

Webster and Tavares suggested using BIC to build a powerful S-Box [27]. Any two output bits should change separately whenever a single input bit is modified, based on the BIC value. This criterion computes both the nonlinearity value. This value should ideally be as high as feasible. It needs to supply the SAC value as well. Table 2 lists the SAC as well as nonlinearity values in the S-Box structures that are suggested for the BIC metric. It can be concluded that this requirement is satisfied because the SAC values are quite near to 0.5. Here, the nonlinearity value has stayed low. Similar to the XOR distribution, this value can also be improved in subsequent research.

4. Audio encryption algorithm

A collection of digitally encrypted audio data are utilised by audio equipment to save, modify, develop, and create sound. Another term for audio in digital form is a collection of discrete sequences that select from the sound wave form. Digital audio signal is essentially made up of discrete terminals that show the digital data wave’s intensity. The study demonstrates how to encrypt the original audio content and modify the separate terminals of the audio format.
The following steps are followed for our proposed scheme:

1. S-Box Array: Initialise the constructed S-Box.
2. Read the Audio File: Its audio file, e.g., (chirp.mat), The.mat file is loaded and the audio data inside it is extracted. Only a single channel (mono) is utilised if the audio happens to be stereo.
3. You add the audio data in floating-point format to an AudioInputStream. This is the step where audio data is converted to single precision and cast it.
4. Audio Data Conversion and Encryption: This refers to converting audio data into bytes, followed by encrypting each byte of the



(a) Chirp

(b) Gong

(c) Handel

(d) Encrypted Chirp

(e) Encrypted Gong

(f) Encrypted Handel

Fig. 1. Wave form of the chirp, gong and handel (a, b, c) original sounds (d, e, f) encrypted signals.

converted audio data as it replaces with an equivalent value from S-Box.

Using above algorithm, the chirp, gong and handel sounds are encrypted. The original and encrypted sounds are represented in wave form in Fig. 1.

5. Analysis of original and cipher audio data

A standard encryption technique must be able to withstand several assaults that aim to compromise the data's secrecy, authenticity, not repudiating, as well as validation. Here, the authors assess the suggested technique's durability and endurance versus various malevolent attacks. On a desktop computer, MATLAB 2018(b) is used for all of these analyses. In order to examine our plan, the authors combine various audio models and apply our suggested method to encrypt these models using several keys. Fig. 1 shows the wave version of the plain and encrypted files. Since the encoded audios are homogeneous in character, it is clear from Fig. 1 that the amplitudes of the actual and encoded audios do not resemble one another. This illustrates how correctly encrypted the audio is. The suggested method is subjected to several analyses in the subsections that follow, including differential analysis, spectogram analysis, as well as key space analysis, among others.

5.1. *Time complexity*

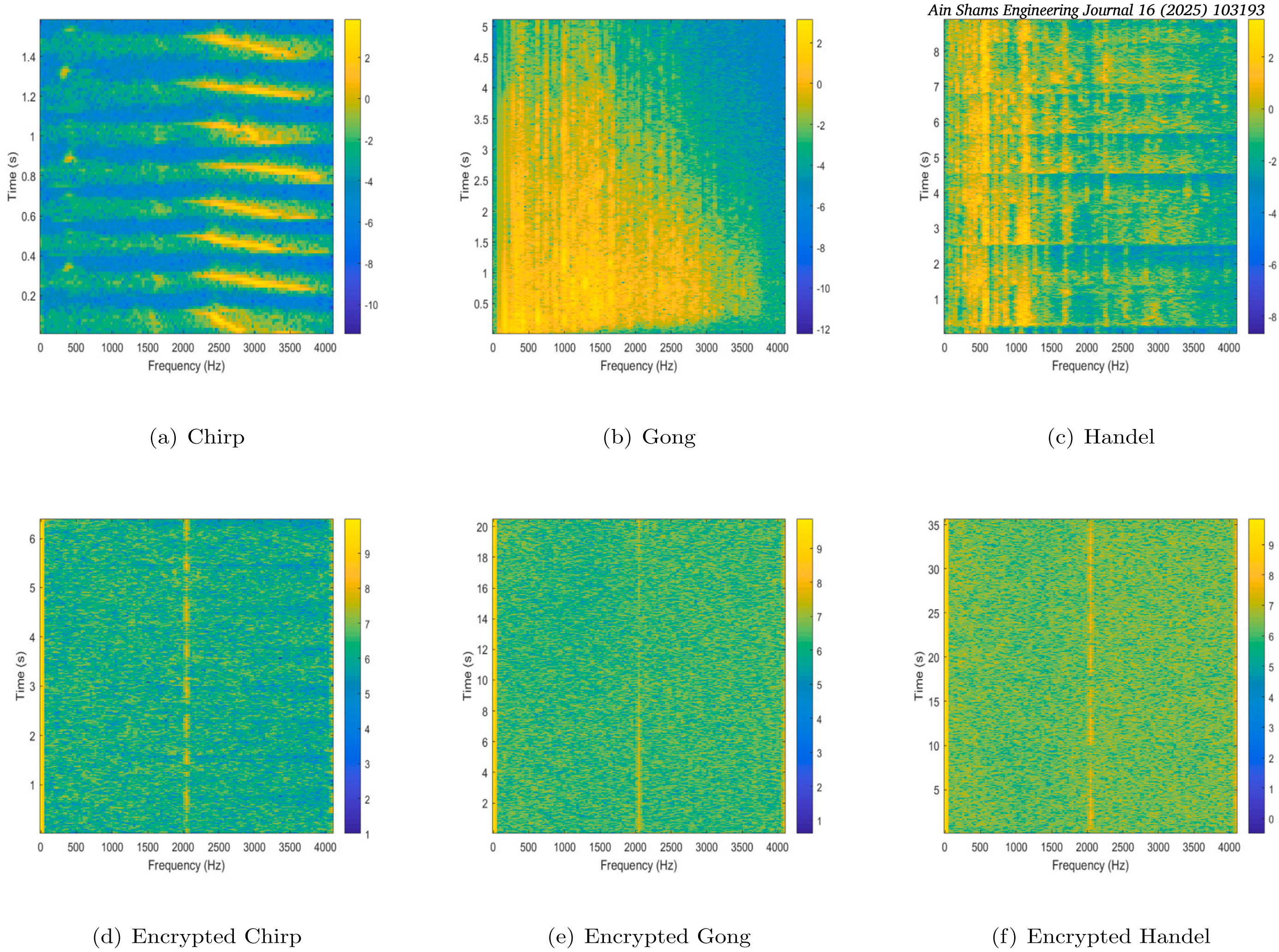
Time complexity in encryption refers to the number of time units an algorithm requires to complete relative to input size. It is one of the essential measures since it directly impacts how fast an encryption technique can encrypt or decrypt, especially if such applications are to be deployed in real-time. For that reason, Big-**O** notation is extensively used to represent time complexity as the measure of how many multiples the runtime grows based on the input size. The time taken for one round of encryption is mentioned in Table 3.

5.2. *Key space analysis*

Large key spaces are necessary for effective encryption techniques to withstand attacks by brute force. The reliability of an encryption technique is directly impacted by the length of the key's space. A trustworthy encryption method must have a minimum key space of 2^{100}. As a result, 256 bits define the space for keys of the recommended strategy, our solution is resistant to all types of attacks that use brute force.

5.3. *Spectogram analysis*

It is advised to employ spectrogram analysis to carry out a spectral examination of sound. This examination is represented as a two-dimensional graph, with the additional dimension being represented by various colours. It is seen as a visual representation of the spectrum's



(a) Chirp

(b) Gong

(c) Handel

(d) Encrypted Chirp

(e) Encrypted Gong

(f) Encrypted Handel

Fig. 2. Spectogram of the chirp, gong and handel (a, b, c) original sounds (d, e, f) encrypted sounds.

varying frequency with respect to time. The hue in the third dimension shows the sound's volume or roughness at a certain moment in time. Blue is used to denote the lowest amplitude, whereas bright signifies the stronger intensity. Fig. 2 presents the findings of our encryption scheme's spectrogram study. The original audio's spectogram shows that the frequency is distributed unevenly. The spectrogram graph of the encoded audio files exhibits regularity, indicating that the encoding is sufficient. This encoded file has a noticeable loudness and a completely different spectrogram from the original audio. Which shows that the encryption scheme provided the high level of authenticity to secure the signal data.

5.4. *Signal to noise ratio*

The "Signal to Noise Ratio (SNR)"is used to measure the quality of the signal. When the value is greater than 0 dB, the signal becomes more than noise. When host as well as encoded audio files are accessible, calculating the SNR is simple. The SNR formula is as follows:

$$SNR = 10 * log_{10} \frac{\sum_{j=1}^{n} \mu_j^2}{\sum_{j=1}^{n} (\mu_j - \nu_j)^2}$$

n is the amount of samples in this case. Additionally, the host's trials and encoded audio files are denoted by μ_j and ν_j. The SNR results of the audio files that were evaluated are shown in Table 3. The scheme's effectiveness is shown by the SNR's value being negative. Table 3 shows that our strategy is more resistant to malicious assaults due to its increased negative SNR.

5.5. *Mean square error and peak signal to noise ratio*

The following formula may be used to determine "the mean squared error"for the two vectors, χ and ξ:

$$MSE = \frac{1}{n} \sum_{\imath=1}^{n} (\chi(\imath) - \xi(\imath))$$

The PSNR can be found as follows if χ displays the host sound file and ξ is its encoded audio file:

$$PSNR = 10 * log_{10} \left(\frac{m^2}{MSE} \right)$$

where m is the stream's maximum value. Table 3 lists the calculated PSNR values for each of the encrypted test audio files. The outcomes are observed to be small. Since lower PSNR values indicate higher noise levels and greater resilience to attacks, it is more advisable to use lower PSNR metrics for encoded audio content. Also, Table 3 contains the time in which encryption process is complete.

5.6. *Differential analysis*

Differential analysis primarily takes into account two types of analyses for differential attacks: "unified average changing intensity

Table 3
SNR, MSE, PSNR and Time analysis.

Voice	SNR	MSE	PSNR (dB)	Time (sec)
Chirp	0.1037	8858.9	8.66	5.018
Gong	0.1768	10451	7.84	3.7313
Handel	0.2890	11791	7.42	5.2998

Table 4
Comparative analysis of NSCR and UACI.

Sounds	NSCR	UACI
Chirp	99.97%	33.31%
Gong	99.99%	33.33%
Handel	99.92%	33.36%
[7]	99.99%	33.34%
[9]	99.65%	33.21%
[4]	99.6124%	33.4176%

(UACI)”and “number of signals change rates (NSCR)”. They determine how sensitive the cryptosystem. A good cryptographic method needs to be sensitive enough that even a small change to the source data results in a large modification in the cipher data. NSCR as well as UACI analysis are commonly used to evaluate the cryptosystem’s sensitivity. “NSCR and UACI”are available as.

$$NSCR = \frac{\sum_{i=1}^{n} \phi(\imath)}{n} \times 100\%$$

where $\phi(\imath)$ can be defined as

$$\phi(\imath) = \begin{cases} 1 \text{ if } M_1(\imath) \neq M_2(\imath) \\ 0 \text{ if } M_1(\imath) = M_2(\imath) \end{cases}$$

$$UACI = \frac{1}{n} \sum_{i=1}^{n} \frac{|M_1(\imath) - M_2(\imath)|}{2^n - 1} \times 100\%$$

where n is the sound signal’s length. The optimal values for “NSCR and UACI”are 100% and 33.33%, respectively. Table 4 states the comparative analysis of our scheme with few latest schemes. This table demonstrates how our technique’s NSCR as well as UACI values are nearly perfect.

6. Conclusion

This study proposes an action over generalised triangle group audio encryption method. The parametrization of the action of the $PSL(2,\mathbb{Z})$ for the triangle groups is extended for $\Delta(2,3,k)$ to the finite generalised triangle groups $\langle u, v \,|u^2 = v^3 = w^k = 1\rangle$ where $w = uvuvuv^2uvuv^2$. Also, based on the resulting parametric equations, the S-Box is constructed which is further used in our audio encryption method. This novel method makes use of the unique features of GTG and its mathematical applications to ensure that the produced S-Boxes have strong cryptographic qualities. Our solution is dependable against these attacks because the suggested methodology functions well and are validated using a range of statistical tests. These durable S-Boxes were created using the suggested technique, and this study plan to employ them in multimedia security applications. Furthermore, the suggested methods for encrypting audio provide comparable or even higher levels of protection when compared to the body of current research. The nonlinearity of the S-Box based on GTG achieved the desired nonlinearity which is 112 on all 8 bits which is considered as strong result. However the highest nonlinearity for 8 bits is 112 then the limitation is that nonlinearity doesn’t exceed 112 in GTG case.

CRediT authorship contribution statement

Aqsa Zafar Abbasi: Writing – original draft, Validation, Methodology, Investigation, Data curation, Conceptualization. **Ayesha Rafiq:** Writing – review & editing, Supervision, Resources, Formal analysis. **Badr M. Alshammari:** Writing – review & editing, Software, Resources, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare no conflict of interest

References

[1] Zafar Abbasi Aqsa, Rafiq Ayesha, Kolsi Lioua. Parametrization of generalized triangle groups and construction of substitution-box for medical image encryption. J King Saud Univ, Comput Inf Sci 2024;36(8):102159.

[2] Ashiq Muhammad, Imran Tahir, Asad Zaighum Muhammad. Actions of △ (3, n, k) on projective line. Trans A Razmadze Math Inst 2018;172(1):1–6.

[3] Baumslag Gilbert, Morgan John W, Shalen Peter B. Generalized triangle groups. Math Proc Camb Philos Soc 1987;102(1):25–31.

[4] Cao Yafei, Liu Hongjun. An audio encryption algorithm based on a non-degenerate 2d integer domain hyper chaotic map over gf (2 n). Multimed Tools Appl 2024:1–20.

[5] Cusick Thomas W, Stanica Pantelimon. Cryptographic Boolean functions and applications. Academic Press; 2017.

[6] Dumas Jean-Guillaume, Orfila Jean-Baptiste. Generating s-boxes from semi-fields pseudo-extensions. arXiv preprint. arXiv:1411.2503, 2014.

[7] Farsana FJ, Devi VR, Gopakumar K. An audio encryption scheme based on fast Walsh Hadamard transform and mixed chaotic keystreams. Appl Comput Inform 2023;19(3/4):239–64.

[8] Fine Benjamin, Howie James, Rosenberger Gerhard. One-relator quotients and free products of cyclics. Proc Am Math Soc 1988;102(2):249–54.

[9] Habib Zeeshan, Khan Jan Sher, Ahmad Jawad, Khan Muazzam A, Khan Fadia Ali. Secure speech communication algorithm via dct and td-ercs chaotic map. In: 2017 4th international conference on electrical and electronic engineering (ICEEE). IEEE; 2017. p. 246–50.

[10] Hagelberg M, Maclachlan C, Rosenberger G. On discrete generalised triangle groups. Proc Edinb Math Soc 1995;38(3):397–412.

[11] Howie James, Metaftsis Vassilis, Thomas Richard M. Finite generalized triangle groups. Trans Am Math Soc 1995;347(9):3613–23.

[12] Hu Yingjie, Zhang Qiuyu, Zhang Qiwen, Ba Yujiao. An intelligent homomorphic audio signal encryption algorithm for secure interacting. Multimed Tools Appl 2024;83(9):25675–93.

[13] Iqtadar Hussain, AmirAnees, TemadherAlassiry Al-Maadeed. A novel encryption algorithm using multiple semifield s-boxes based on permutation of symmetric group. Comput Appl Math 2023;42(2):80.

[14] Hussain Sadam, Jamal Sajjad Shaukat, Shah Tariq, Hussain Iqtadar. A power associative loop structure for the construction of non-linear components of block cipher. IEEE Access 2020;8:123492–506.

[15] Hussain Sadam, Shah Tariq, Javeed Adnan. Modified advanced encryption standard (maes) based on non-associative inverse property loop. Multimed Tools Appl 2023;82(11):16237–56.

[16] Tahir Imran, Ashiq Muhammad, Asad Zaighum Muhammad. Computational approach for intransitive action of △ (2, 4,k) on $PL(F_q)$. Quasigr Relat Syst 2020;28(1):139–48.

[17] Levin F, Rosenberger G. On free subgroups of generalized triangle groups, part ii. Group Theory World Sci 1993:206–28.

[18] Mustaq Q. Parametrization of all homomorphisms from $\mathrm{PGL}(2,\mathbb{Z})$ into $\mathrm{PGL}(2,q)$. Commun Algebra 1992;20(4):1023–40.

[19] Rafiq Ayesha, Khan Majid. Construction of new s-boxes based on triangle groups and its applications in copyright protection. Multimed Tools Appl 2019;78(11):15527–44.

[20] Razaq Abdul, Ahmad Musheer, Abd El-Latif Ahmed A. A novel algebraic construction of strong s-boxes over double gf (27) structures and image protection. Comput Appl Math 2023;42(2):90.

[21] Servetti Antonio, Carlos De Martin Juan. Perception-based partial encryption of compressed speech. IEEE Trans Speech Audio Process 2002;10(8):637–43.

[22] Dawood Shah, Shah Tariq, Mazyad Hazzazi Mohammad, Imran Haider Muhammad, Aljaedi Amer, Hussain Iqtadar. An efficient audio encryption scheme based on finite fields. IEEE Access 2021;9:144385–94.

[23] Dawood Shah, Shah Tariq, Jamal Sajjad Shoukat. Digital audio signals encryption by mobius transformation and Hénon map. Multimed Syst 2020;26(2):235–45.

[24] Nasir Siddiqui, Yousaf Fahim, Murtaza Fiza, Ehatisham-ul Haq Muhammad, Usman Ashraf M, Alghamdi Ahmed M, et al. A highly nonlinear substitution-box (s-box) design using action of modular group on a projective line over a finite field. PLoS ONE 2020;15(11):e0241890.

[25] Thorwirth NJ, Horvatic P, Weis R, Zhao Jian. Security methods for mp3 music delivery. Conference record of the thirty-fourth asilomar conference on signals, systems and computers (Cat. No. 00CH37154), vol. 2. IEEE; 2000. p. 1831–5.

[26] Vinberg Ernest Borisovich, Kaplinsky Y. Pseudo-finite generalized triangle groups. Sonderforschungsbereich, vol. 343. 2000.

[27] Webster Arthur F, Tavares Stafford E. On the design of s-boxes. In: Conference on the theory and application of cryptographic techniques. Springer; 1985. p. 523–34.