




# Vectrix: A Proposed Mathematical Structure and Its Application in Cryptography

Abdulkadir Datti<sup>1</sup>

<sup>1</sup>Department of Mathematical Sciences, Faculty of Science, Sa'adu Zungur University, Bauchi State, Nigeria.

\*Correspondence: [adatti@sazu.edu.ng](mailto:adatti@sazu.edu.ng)

Abstract	Article History
<p>This paper studies the security of the Hill cipher through its key space and the entropy of the keys, the analysis was extended to a proposed structure called Vectrix (plural, Vectrices). The key space of the existing cipher is define by the space of non-singular matrices, and for the proposed algorithm it is define by the space of non-singular Vectrices. In each case, Shannon entropy was used to measure the associated uncertainty. The results shows that, the entropy associated with Vectrix key is triple of the entropy of the traditional Hill Cipher key and the key space is cubic power of the key space of the respective Matrix key space.</p>	<p>Received: 10/04/2025 Accepted: 22/06/2025 Published: 30/06/2025</p>
	<p><b>Keywords:</b> Encryption; Decryption; Hill-Cipher; Cryptography; vectrix; Shannon entropy</p>
	<p><b>License:</b> CC BY 4.0*</p>  <p><b>Open Access Article</b></p>
<p><b>How to cite this paper:</b> Datti, A. (2025). Vectrix: A Proposed Mathematical Structure and Its Applications in Cryptography. <i>Gadua J Pure Alli Sci</i>, 4(1): 19-26. <a href="https://doi.org/10.54117/w5x30d53">https://doi.org/10.54117/w5x30d53</a></p>	

## 1.0 Introduction

Mathematics plays a vital role in diverse fields of knowledge and practical applications, one of which is securing sensitive information. The earliest known use of cryptography dates back thousands of years, when Julius Caesar introduced a substitution method to encode military messages. Although effective at the time, this method was vulnerable to frequency analysis, which leads to the development of advanced algorithms. Among these is the Hill Cipher, introduced in 1929 (Hassan et al., 2022; Ameen et al., 2025; Perna et al., 2014) where encryption is performed using a key matrix and decryption by the inverse. A basic requirement is that the key matrix be invertible and its determinant be relatively prime to the chosen modulus. If either the matrix or its inverse is known, the cipher-text can be easily decoded. Subsequent studies analyzed and attempted to strengthen the Hill Cipher. For example, Overbey,

Traves, and Wojdylo investigated the size of the key space and proposed the use of involutory matrices Overbey et al. (2005). However, the smaller size of the space compared to the full set of invertible matrices limit its effectiveness. They also showed that the order of the key space increases with key dimension, and that prime moduli yield larger key spaces than composite ones. Other modifications attempt to counteract vulnerabilities such as known-plaintext attacks and its poor performance on images with uniform color. One approach introduced random key matrices for each block of text (Ismail et al., 2006; Jain & Aryan, 2022) while another use row and column permutations (Saeednia, 2009). Hybrid algorithms have also been developed, such as combining the Hill Cipher with Caesar Cipher (Qowi & Hudallah, 2021), or with a modified sigmoid function for generating multiple keys (Mfungo et al, 2023). Santoso (2021) proposed a combined Hill–

\*Journal of the Faculty of Science, Bauchi State University Gadua, Nigeria

MATS – Mathematical Sciences

This work is published open access under the [Creative Commons Attribution License 4.0](https://creativecommons.org/licenses/by/4.0/), which permits free reuse, remix, redistribution and transformation provided due credit is given

SRA system where both the key and the message are encrypted.

In this study, we introduce a different method by constructing a new algebraic structure, termed the Vectrix (plural, Vectrices). Vectrix key is defined as a triplet of independent invertible matrices whose determinants are pairwise relatively prime to the encryption modulus. This construction provides a key consisting of three independent subkeys, thereby improving the security. It is expected that applying Vectrix-based method to existing Hill Cipher modifications would provide stronger protection.

## 2.0 Basic Definition

In this section, we introduce the definition of a Vectrix and describe the basic operations associated with it.

### Definition 2.1

Let  $A_1$ ,  $A_2$  and  $A_3$  be matrices of the same order. A Vectrix  $\vec{A}$  is defined as

$\vec{A} = A_1 i + A_2 j + A_3 k$ . Where  $A_1$ ,  $A_2$  and  $A_3$  are the **components** of the Vectrix, and  $i$ ,  $j$  and  $k$  denote the **classes** of the components.

If all component matrices are zero matrices, then  $\vec{A}$  is called a **zero Vectrix**; if all component matrices are identity matrices, it is called identity **Vectrix**. A **square Vectrix** is one whose component matrices are square.

Since matrices are typically denoted by capital letters, Vectrices will be denoted by capital letters with an arrow head.

### Definition 2.2

The **order** of a Vectrix is the common order of its component matrices.

The **addition** of Vectrices is defined componentwise. That is, if

$\vec{A} = A_1 i + A_2 j + A_3 k$  and  $\vec{B} = B_1 i + B_2 j + B_3 k$  then

$$\vec{A} + \vec{B} = (A_1 + B_1)i + (A_2 + B_2)j + (A_3 + B_3)k$$

**Scalar multiplication** is defined similar to scalar multiplication of vectors and matrices.

### Definition 2.3

If  $\vec{A}$  and  $\vec{B}$  are Vectrices such that the matrix multiplications  $A_1 B_1$ ,  $A_2 B_2$  and  $A_3 B_3$  are defined, then the **Vectrix-multiplication** is defined by

$$\vec{A} \otimes \vec{B} = A_1 B_1 i + A_2 B_2 j + A_3 B_3 k$$

### Definition 2.4

The **determinant** of a Vectrix  $\vec{A} = A_1 i + A_2 j + A_3 k$  is a vector defined as

$$|\vec{A}| = |A_1| i + |A_2| j + |A_3| k$$

As in the case of matrices, the determinant exists if and only if it is a square Vectrix. A Vectrix is **singular** if its determinant is zero and **invertible** if its determinant is nonzero. A square Vectrix has an inverse if and only if it is invertible. The **inverse** of a Vectrix  $\vec{A} = A_1 i + A_2 j + A_3 k$  is a Vectrix  $\vec{B} = B_1 i + B_2 j + B_3 k$  whose determinant is

$$|\vec{B}| = \left| \frac{1}{A_1} \right| i + \left| \frac{1}{A_2} \right| j + \left| \frac{1}{A_3} \right| k$$

## 3.0 Results

In this section, we present the Hill Cipher algorithm using a matrix as the key, and its modification using a Vectrix as the key. Similar to the key matrix, a key Vectrix must be invertible, and each component of its determinant vector must be relatively prime to the chosen modulus. Finally, we illustrate both methods with a numerical example.

### 3.1 Hill-Cipher Algorithm Using Matrix Key

#### A. Encryption Process

1. Break the original text into a number of subtexts of equal length. Complete the last subtext with spacing characters if necessary.
2. Convert each subtext to its numeric equivalent and present it as a column vector.
3. Modula-multiply each resulting vector by the key matrix to encrypt the vectors.
4. Generate the encrypted subtexts from the encrypted vectors.

#### B. Decryption Process

1. Convert the encrypted subtexts to their numeric equivalents to retrieve the encrypted vectors.
2. Modula-multiply each vector by the inverse of the key matrix to decrypt them.
3. Convert the components of each decrypted vector back to alphanumeric characters to generate the original subtexts.

### 3.2 Hill-Cipher Algorithm Using Vectrix Key

#### A. Encryption Process

1. Break the original text into three groups of subtexts of equal length. Split each group into smaller subtexts of equal length. Complete the last subtext in each group with spacing characters if necessary.
2. Convert each smaller subtext to its numeric equivalent and present it as a column vector.
3. Construct Vectrices from the column vectors. Each Vectrix should have components drawn from the respective subtext group.
4. Modulo-multiply each resulting Vectrix by the corresponding key Vectrix to encrypt them.
5. Generate the encrypted text from the encrypted Vectrices.

#### B. Decryption Process

1. Convert the encrypted text to numeric equivalents to retrieve the encrypted Vectrices.
2. Modulo-multiply each Vectrix by the inverse of the key Vectrix to decrypt them.
3. Extract three sets, each consisting of the respective components of the decrypted Vectrices.
4. Convert each set to alphanumeric characters and concatenate them to reconstruct the original text.

#### 3.3 Numerical Example

Use the statement "Encryption using matrix-key and using Vectrix-key" to illustrate the two algorithms.

##### 3.3.1 Solution using Matrix key algorithm:

Consider the following table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z		?
16	17	18	19	20	21	22	23	24	25	26	27	28

#### A. Encryption process

1. We, first break the text into subtexts of three characters as follows:  
(ENC), (RYP), (TIO), (N U), (SIN), (G M), (ATR), (IX-), (KEY), ( AN), (D U), (SIN), (G V) , (ECT), (ORI), (X-K), (EY).
2. Next, we convert each subtext to numeric vectors as follows:

$$\begin{pmatrix} 5 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 18 \\ 25 \\ 16 \end{pmatrix}, \begin{pmatrix} 20 \\ 9 \\ 15 \end{pmatrix}, \begin{pmatrix} 14 \\ 27 \\ 21 \end{pmatrix}, \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix}, \begin{pmatrix} 7 \\ 27 \\ 13 \end{pmatrix}, \begin{pmatrix} 1 \\ 20 \\ 18 \end{pmatrix}, \begin{pmatrix} 9 \\ 24 \\ 29 \end{pmatrix},$$

$$\begin{pmatrix} 11 \\ 5 \\ 25 \end{pmatrix}, \begin{pmatrix} 27 \\ 1 \\ 14 \end{pmatrix}, \begin{pmatrix} 4 \\ 27 \\ 21 \end{pmatrix}, \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix}, \begin{pmatrix} 7 \\ 27 \\ 22 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \\ 20 \end{pmatrix}, \begin{pmatrix} 15 \\ 18 \\ 9 \end{pmatrix}, \begin{pmatrix} 24 \\ 29 \\ 11 \end{pmatrix},$$

$$\begin{pmatrix} 5 \\ 25 \\ 27 \end{pmatrix}$$

3. Then, we multiply each of resulting vectors modulo 29 by a key-matrix

$$\begin{pmatrix} 1 & 0 & 1 \\ 3 & 1 & 2 \\ 0 & 0 & 7 \end{pmatrix}$$

to get the following encrypted vectors

$$\begin{pmatrix} 8 \\ 6 \\ 21 \end{pmatrix}, \begin{pmatrix} 5 \\ 24 \\ 25 \end{pmatrix}, \begin{pmatrix} 6 \\ 12 \\ 18 \end{pmatrix}, \begin{pmatrix} 6 \\ 24 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \\ 11 \end{pmatrix}, \begin{pmatrix} 20 \\ 16 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 1 \\ 10 \end{pmatrix}, \begin{pmatrix} 9 \\ 22 \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} 7 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 12 \\ 23 \\ 11 \end{pmatrix}, \begin{pmatrix} 25 \\ 23 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \\ 11 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 9 \end{pmatrix}, \begin{pmatrix} 25 \\ 0 \\ 24 \end{pmatrix}, \begin{pmatrix} 24 \\ 23 \\ 5 \end{pmatrix}, \begin{pmatrix} 6 \\ 7 \\ 19 \end{pmatrix},$$

$$\begin{pmatrix} 3 \\ 7 \\ 15 \end{pmatrix}$$

4. Finally, we obtain the following encrypted subtexts:

(HFU), (EXY), (FLR), (FXB), (DGK), (TPD), (SAJ), (IV-), (GAA), (LWK), (YWB), (DGK), (-EI), (Y-X), (XWE), (FGS), (CGO).

This leads to the following encrypted text

"HFUEXYFLRFXBDGKTPDSAIV-  
GAALWKYWBDGK-EIY-XXWFGSCGO"

#### B. Decryption Process

1. We initiate the decryption process by converting the encrypted subtexts:  
(HFU), (EXY), (FLR), (FXB), (DGK), (TPD), (SAJ), (IV-), (GAA), (LWK), (YWB), (DGK), (-EI), (Y-X), (XWE), (FGS), (CGO).  
to the followin vectors:

$$\begin{pmatrix} 8 \\ 6 \\ 21 \end{pmatrix} \begin{pmatrix} 5 \\ 24 \\ 25 \end{pmatrix} \begin{pmatrix} 6 \\ 12 \\ 18 \end{pmatrix}, \begin{pmatrix} 6 \\ 24 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \\ 11 \end{pmatrix}, \begin{pmatrix} 20 \\ 16 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 1 \\ 10 \end{pmatrix}, \begin{pmatrix} 9 \\ 22 \\ 0 \end{pmatrix}, \\ \begin{pmatrix} 7 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 12 \\ 23 \\ 11 \end{pmatrix}, \begin{pmatrix} 25 \\ 23 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \\ 11 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 9 \end{pmatrix}, \begin{pmatrix} 25 \\ 0 \\ 24 \end{pmatrix}, \begin{pmatrix} 24 \\ 23 \\ 5 \end{pmatrix}, \begin{pmatrix} 6 \\ 7 \\ 19 \end{pmatrix}, \\ \begin{pmatrix} 3 \\ 7 \\ 15 \end{pmatrix}$$

2. Then, we multiply each of resulting vectors modulo 29 by the inverse of the key-matrix,

$$\begin{pmatrix} 1 & 0 & -\frac{1}{7} \\ 3 & 1 & \frac{1}{7} \\ 0 & 0 & \frac{1}{7} \end{pmatrix}$$

to get the following decrypted the vectors:

$$\begin{pmatrix} 5 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 18 \\ 25 \\ 16 \end{pmatrix} \begin{pmatrix} 20 \\ 9 \\ 15 \end{pmatrix}, \begin{pmatrix} 14 \\ 27 \\ 21 \end{pmatrix}, \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix}, \begin{pmatrix} 7 \\ 27 \\ 13 \end{pmatrix}, \begin{pmatrix} 1 \\ 20 \\ 18 \end{pmatrix}, \\ \begin{pmatrix} 9 \\ 24 \\ 29 \end{pmatrix}, \begin{pmatrix} 11 \\ 5 \\ 25 \end{pmatrix}, \begin{pmatrix} 27 \\ 1 \\ 14 \end{pmatrix}, \begin{pmatrix} 4 \\ 27 \\ 21 \end{pmatrix}, \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix}, \begin{pmatrix} 7 \\ 27 \\ 22 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \\ 20 \end{pmatrix}, \\ \begin{pmatrix} 15 \\ 18 \\ 9 \end{pmatrix}, \begin{pmatrix} 24 \\ 29 \\ 11 \end{pmatrix}, \begin{pmatrix} 5 \\ 25 \\ 27 \end{pmatrix}.$$

3. Finally, we obtain the following decrypted subtexts:

(ENC), (RYP), (TIO), (N U), (SIN), (G M), (ATR), (IX-), (KEY), ( AN), (D U), (SIN), (G V) , (ECT), (ORI), (X-K), (EY ),

from which we have the original text "Encryption using matrix-key and using Vectrix-key"

### 3.3.2 Solution using vectrix key algorithm:

#### A. Encryption process

1. We first break the original text into the following subtexts:

$T_1$  = ENCRYPTION USING,

$T_2$  = MATRIX-KEY AND US ,

$T_3$  = ING VECTORIX-KEY .

This leads to the following groups of smaller subtexts "(ENC), (RYP), (TIO), (N U), (SIN), (G )", "(MAT), (RIX), (-KE), (Y A), (ND ) (US )" and "(ING), ( VE), (CTO), (RIX), (-KE), (Y )" "

2. Then we have the following sets of vectors

$$S_1 = \left\{ \begin{pmatrix} 5 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 18 \\ 25 \\ 16 \end{pmatrix}, \begin{pmatrix} 20 \\ 9 \\ 15 \end{pmatrix}, \begin{pmatrix} 14 \\ 27 \\ 21 \end{pmatrix}, \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix}, \begin{pmatrix} 7 \\ 27 \\ 13 \end{pmatrix} \right\}, \\ S_2 = \left\{ \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix}, \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix}, \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix}, \begin{pmatrix} 25 \\ 27 \\ 1 \end{pmatrix}, \begin{pmatrix} 14 \\ 4 \\ 27 \end{pmatrix}, \begin{pmatrix} 21 \\ 19 \\ 27 \end{pmatrix} \right\} \text{ and} \\ S_3 = \left\{ \begin{pmatrix} 9 \\ 14 \\ 7 \end{pmatrix}, \begin{pmatrix} 27 \\ 22 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 20 \\ 15 \end{pmatrix}, \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix}, \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix}, \begin{pmatrix} 25 \\ 27 \\ 27 \end{pmatrix} \right\}$$

3. Next, we construct the following Vectrices:

$$A = \begin{pmatrix} 5 \\ 14 \\ 3 \end{pmatrix} i + \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix} j + \begin{pmatrix} 9 \\ 14 \\ 7 \end{pmatrix} k \\ B = \begin{pmatrix} 18 \\ 25 \\ 16 \end{pmatrix} i + \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix} j + \begin{pmatrix} 27 \\ 22 \\ 5 \end{pmatrix} k \\ C = \begin{pmatrix} 20 \\ 9 \\ 15 \end{pmatrix} i + \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix} j + \begin{pmatrix} 3 \\ 20 \\ 15 \end{pmatrix} k \\ D = \begin{pmatrix} 14 \\ 27 \\ 21 \end{pmatrix} i + \begin{pmatrix} 25 \\ 27 \\ 1 \end{pmatrix} j + \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix} k \\ F = \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix} i + \begin{pmatrix} 14 \\ 4 \\ 27 \end{pmatrix} j + \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix} k \text{ and} \\ G = \begin{pmatrix} 7 \\ 27 \\ 27 \end{pmatrix} i + \begin{pmatrix} 21 \\ 19 \\ 27 \end{pmatrix} j + \begin{pmatrix} 25 \\ 27 \\ 27 \end{pmatrix} k$$

4. Finally, we Modula-multiply each of the above Vectrix by a key-Vectrix

$$\begin{pmatrix} 1 & 0 & 1 \\ 3 & 1 & 2 \\ 0 & 0 & 7 \end{pmatrix} i + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} j + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} k$$

to get the following encrypt Vectrices

$$A = \begin{pmatrix} 8 \\ 6 \\ 21 \end{pmatrix} i + \begin{pmatrix} 13 \\ 1 \\ 11 \end{pmatrix} j + \begin{pmatrix} 9 \\ 13 \\ 7 \end{pmatrix} k$$

$$B = \begin{pmatrix} 5 \\ 24 \\ 25 \end{pmatrix} i + \begin{pmatrix} 18 \\ 9 \\ 19 \end{pmatrix} j + \begin{pmatrix} 27 \\ 8 \\ 5 \end{pmatrix} k$$

$$C = \begin{pmatrix} 6 \\ 12 \\ 18 \end{pmatrix} i + \begin{pmatrix} 29 \\ 11 \\ 10 \end{pmatrix} j + \begin{pmatrix} 3 \\ 2 \\ 15 \end{pmatrix} k$$

$$D = \begin{pmatrix} 6 \\ 24 \\ 2 \end{pmatrix} i + \begin{pmatrix} 25 \\ 27 \\ 2 \end{pmatrix} j + \begin{pmatrix} 18 \\ 27 \\ 24 \end{pmatrix} k$$

$$F = \begin{pmatrix} 4 \\ 7 \\ 11 \end{pmatrix} i + \begin{pmatrix} 14 \\ 4 \\ 25 \end{pmatrix} j + \begin{pmatrix} 29 \\ 4 \\ 5 \end{pmatrix} k$$

$$G = \begin{pmatrix} 5 \\ 15 \\ 13 \end{pmatrix} i + \begin{pmatrix} 21 \\ 19 \\ 25 \end{pmatrix} j + \begin{pmatrix} 25 \\ 23 \\ 27 \end{pmatrix} k$$

4. this results to the following encrypted text "HFUMAKIMGEXYRIS HEFLR-KJCBOFXBY BR XDGKNDY-DEEOMUSYYW "

#### B. Decryption Process

1. The numeric equivalent of "HFUMAKIMGEXYRIS HEFLR-KJCBOFXBY BR XDGKNDY-DEEOMUSYYW " is "8,6,21,13,1,11,9,13,7,5,24,25,18,9,19,27,8,56,12,18, 29,11,10,3,2,15,6,24,2,25,27,2,18,27,24,4,7,11,14,4,2 5,29,4,5,5,15,13,21,19,25,25,23,27". This results to the following vectories

$$A = \begin{pmatrix} 8 \\ 6 \\ 21 \end{pmatrix} i + \begin{pmatrix} 13 \\ 1 \\ 11 \end{pmatrix} j + \begin{pmatrix} 9 \\ 13 \\ 7 \end{pmatrix} k$$

$$B = \begin{pmatrix} 5 \\ 24 \\ 25 \end{pmatrix} i + \begin{pmatrix} 18 \\ 9 \\ 19 \end{pmatrix} j + \begin{pmatrix} 27 \\ 8 \\ 5 \end{pmatrix} k$$

$$C = \begin{pmatrix} 6 \\ 12 \\ 18 \end{pmatrix} i + \begin{pmatrix} 29 \\ 11 \\ 10 \end{pmatrix} j + \begin{pmatrix} 3 \\ 2 \\ 15 \end{pmatrix} k$$

$$D = \begin{pmatrix} 6 \\ 24 \\ 2 \end{pmatrix} i + \begin{pmatrix} 25 \\ 27 \\ 2 \end{pmatrix} j + \begin{pmatrix} 18 \\ 27 \\ 24 \end{pmatrix} k$$

$$F = \begin{pmatrix} 4 \\ 7 \\ 11 \end{pmatrix} i + \begin{pmatrix} 14 \\ 4 \\ 25 \end{pmatrix} j + \begin{pmatrix} 29 \\ 4 \\ 5 \end{pmatrix} k$$

$$G = \begin{pmatrix} 5 \\ 15 \\ 13 \end{pmatrix} i + \begin{pmatrix} 21 \\ 19 \\ 25 \end{pmatrix} j + \begin{pmatrix} 25 \\ 23 \\ 27 \end{pmatrix} k$$

2. Multiplying the vectories modulo 29 by the inverse of the key-Vectrix

$$\begin{pmatrix} 1 & 0 & -25 \\ -3 & 0 & 25 \\ 0 & 0 & 25 \end{pmatrix} i + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} j + \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix} k$$

we have the following decrypted Vectrices

$$A = \begin{pmatrix} 5 \\ 14 \\ 3 \end{pmatrix} i + \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix} j + \begin{pmatrix} 9 \\ 14 \\ 7 \end{pmatrix} k$$

$$B = \begin{pmatrix} 18 \\ 25 \\ 16 \end{pmatrix} i + \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix} j + \begin{pmatrix} 27 \\ 22 \\ 5 \end{pmatrix} k$$

$$C = \begin{pmatrix} 20 \\ 9 \\ 15 \end{pmatrix} i + \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix} j + \begin{pmatrix} 3 \\ 20 \\ 15 \end{pmatrix} k$$

$$D = \begin{pmatrix} 14 \\ 27 \\ 21 \end{pmatrix} i + \begin{pmatrix} 25 \\ 27 \\ 1 \end{pmatrix} j + \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix} k$$

$$F = \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix} i + \begin{pmatrix} 14 \\ 4 \\ 27 \end{pmatrix} j + \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix} k$$

and

$$G = \begin{pmatrix} 7 \\ 27 \\ 27 \end{pmatrix} i + \begin{pmatrix} 21 \\ 19 \\ 27 \end{pmatrix} j + \begin{pmatrix} 25 \\ 27 \\ 27 \end{pmatrix} k$$

3. This leads to the following sets

$$S_1 = \left\{ \begin{pmatrix} 5 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 18 \\ 25 \\ 16 \end{pmatrix}, \begin{pmatrix} 20 \\ 9 \\ 15 \end{pmatrix}, \begin{pmatrix} 14 \\ 27 \\ 21 \end{pmatrix}, \begin{pmatrix} 19 \\ 9 \\ 14 \end{pmatrix}, \begin{pmatrix} 7 \\ 27 \\ 27 \end{pmatrix} \right\}$$

$$S_2 = \left\{ \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix}, \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix}, \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix}, \begin{pmatrix} 25 \\ 27 \\ 1 \end{pmatrix}, \begin{pmatrix} 14 \\ 4 \\ 27 \end{pmatrix}, \begin{pmatrix} 21 \\ 19 \\ 27 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} 9 \\ 14 \\ 7 \end{pmatrix}, \begin{pmatrix} 27 \\ 22 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 20 \\ 15 \end{pmatrix}, \begin{pmatrix} 18 \\ 9 \\ 24 \end{pmatrix}, \begin{pmatrix} 29 \\ 11 \\ 5 \end{pmatrix}, \begin{pmatrix} 25 \\ 27 \\ 27 \end{pmatrix} \right\}$$

4. Finally we have the following alpha numeric sets

$$S_1 = \{ ENC, RYP, TIO, NU, \sin, G \},$$

$$S_2 = \{ MAT, RIX, -KE, YA, ND, US \}$$

and

$$S_3 = \{ ING, VE, CTO, RIX, -KE, Y \}$$

These give the original text "Encryption using key-matrix and using key-vectrix"

#### 4.0 Key-Space and Entropy of the Algorithm}

The security of symmetric-key ciphers is influenced by the size of their key space, as the resistance to exhaustive search attacks depends on it. For the Hill cipher, the key space is defined by the set of all key matrices over a finite set. The randomness of the key defines the rate of its uncertainty; to quantify this, Shannon entropy has been employed (Shannon, 1949). This section outlines the derivation of the Hill cipher key space and its entropy by enumerating matrices and their invertible subsets, then extending the result to Vectrices.

##### Definition 4.1

Let  $F_q$  be a finite field with  $q$  elements. An *mbyn* matrix over  $F_q$  is an array whose entries are independently chosen from  $F_q$ . Since each entry can take  $q$  possible values, the total number of such matrices is  $|M_{(m,n)}| = q^{mn}$ .

This represents the cardinality of the space of all *mbyn* matrices regardless of the invertibility. Not all square matrices of order  $n$  are suitable as Hill cipher keys, the key must be invertible for encryption and decryption to be possible

##### Definition 4.2

Let  $GL_n(F_q)$  be a **general linear group**, that is, the set of invertible *nbyn* matrices over  $F_q$ . The cardinality  $GL_n(F_q)$  is defined by:

$$|GL_n(F_q)| = \prod_{i=0}^{n-1} (q^n - q^i)$$

This is due to the fact that the first column can be any nonzero vector in  $F_q^n$  (giving  $q^n - 1$  possible options), the second column any vector linearly independent of the first ( $q^n - q$  possible options), and so on, until the  $n^{th}$  column. This product gives the exact number of invertible matrices and hence the exact key space of the cipher. The definition was extended to Vectrices as follows:

##### Definition 4.3

Let  $F_q$  be a finite field with  $q$  elements and let  $M_{(m,n)}$  be the set of all *mbyn* matrices over  $F_q$ . An *mbyn* Vectrix over  $F_q$  is a vector whose components chosen from  $M_{(m,n)}$ . Since each entry can take  $q^{mn}$  possible values, the total number of such Vectrices is  $|V_{m,n}| = q^{3mn}$ .

This gives the cardinality of the space of all  $m$  by  $n$  Vectrices.

##### Definition 4.4

Let  $QL_n(F_q)$  be a set of all *nbyn* invertible Vectrices under Vectrix-multiplication define by  $\vec{A} \otimes \vec{B} = A_1 B_1 i + A_2 B_2 j + A_3 B_3 k$ , then  $QL_n(F_q)$  is a group with cardinality defined by:

$$|QL_n(F_q)| = \left( \prod_{i=0}^{n-1} (q^n - q^i) \right)^3$$

It is easy to prove that  $QL_n(F_q)$  is a group. This shows that the key space of the Hill Cipher using the proposed algorithm is cubic of the matrix key space of the same order. Next we compute the entropy of the algorithms using the Shannon entropy measurement.

##### Definition 4.4:

Shannon entropy is a measure of uncertainty in a random variable. For a discrete random variable  $X$  with possible outcomes  $x_1, x_2, \dots, x_n$  and corresponding probabilities  $p(x_1), p(x_2), \dots, p(x_n)$  the entropy  $E(X)$  is defined by:  $E(X) = -\sum p(x_i) \log_2 p(x_i)$ .

If one outcome is certain, then entropy is zero. If all outcomes are equally likely, i.e.,  $p(x_i) = \frac{1}{n}$ , then

$$\text{entropy: } E(X) = \log_2 n.$$

##### Definition 4.5:

Consider a Hill cipher in which a block size  $n$  and  $m$  alphabets are used.

If keys are chosen uniformly at random from all invertible *nbyn* matrices modulo  $m$ , then the key entropy is given by  $E = \log_2 |GL_n(F_q)|$



**Definition 4.6:**

Consider a Hill cipher in which a block size  $n$  and  $m$  alphabets are used. If keys are chosen uniformly at random from all invertible  $n$ byn Vectrices modulo  $m$ , then the key entropy is given by

$$E = \log_2 |QL_n(F_q)| = 3 \log_2 |GL_n(F_q)|$$

**Table I: Matrix Hill Cipher versus Vectrix Hill Cipher**

S/No	MATRIX METHOD	Vectrix METHOD
1	The key space is a cube root of the space of the invertible Vectrices	The key space is a cube of the space of invertible matrices
2	The entropy of a key is one-third of the entropy of the Vectrix key	The entropy of a key triples the entropy of the matrix key

**5.0 Conclusion**

In this paper a brief study of the Hill-Cipher using the existing approach and a modified algorithm has been presented. The modified method was generated by replacing the key-matrix with a key-Vectrix, based on the presented results, although the modified algorithm is not absolutely secured but it has higher security compared to the existing cipher. It is probable that improving the current method could lead to absolutely secured cryptographic algorithm, and replacing key-matrix with key-Vectrix in any of the existing modifications of the Hill Cipher add to the security of the information. Additionally, the present work could be a starting point for extensive study of Vectrices, which is expected to be highly applicable in various fields of science and technology. Future research will be focused on using Vectrix in various cryptographic settings where matrices were used as keys, applying Vectrix method to construct determinants for rectangular matrices and using the matrices in cryptographic algorithms. Finally, additional properties and operation over Vectrix could be developed, and this will lead to the construction of additional operations over matrices,

such as piecewise multiplication, piecewise addition and so on.

**Acknowledgment**

This research was supported by the Tertiary Education Trust Fund (TETFund), Nigeria, through the Institution-Based Research (IBR) intervention at Sa'adu Zungur University, Gadau (Bauchi State University Gadau).

**Declarations****Competing interests**

The author declare that he has no competing interests.

**Ethics approval and consent to participate**

Not applicable

**Authors' contributions**

Not applicable

**Authors' information**

Abdulkadir Datti is Lecturer I in the Department of Mathematical Sciences, Sa'adu Zungur University Gadau. Bauchi state Nigeria

**Consent for publication**

The author has read and consented to the publication of the manuscript.

**Availability of data and material**

Not Applicable.

**Funding**

Funding was obtained from the Tertiary Education Trust Fund (TETFund) Nigeria for project funding under the Institutional-Base Research (IBR) grant.

**References**

- Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4), 656–715. <https://doi.org/10.1002/j.1538-7305.1949.tb00928.x>
- Mfungo, D. E., Fu, X., Wang, X., & Xian, Y. (2023). Enhancing image encryption with the Kronecker XOR product, the Hill cipher, and the sigmoid logistic map. *Applied Sciences*, 13(6), 4034. <https://doi.org/10.3390/app13064034>
- Ismail, I. A., Amin, M., & Diab, H. (2006). How to repair the Hill cipher. *Journal of Zhejiang*

- University Science A, 7(12), 2022–2030.  
<https://doi.org/10.1631/jzus.2006.A2022>
- Overbey, J., Traves, W., & Wojdylo, J. (2005). On the keyspace of the Hill cipher. *Cryptologia*, 29(1), 59–72. <https://doi.org/10.1080/0161-110591893771>
- Hassan, K. A., Garko, A., Sani, S., Abdullahi, U., & Sahalu, S. (2022). Combined techniques of Hill cipher and transposition cipher. *Journal of Mathematical Letters*, 1(1), 57–64. <https://doi.org/10.31586/jml.2023.822>
- Ameen, K. A., Abdulwahab, W. K., & Taher, Y. N. A. (2025). Encryption technique using a mixture of Hill cipher and modified DNA for secure data transmission. *International Journal of Computing and Digital Systems*, 17(2), 1–9. <https://doi.org/10.12785/ijcds/1571016767>
- Prerna, Urooj, M., Kumari, M., & Shrivastava, J. N. (2014). Image encryption and decryption using modified Hill cipher technique. *International Journal of Information and Computation Technology*, 4(17), 1895–1901. <https://www.ripublication.com/>  
[ijictv4n17spl\\_20.pdf](https://www.ripublication.com/ijictv4n17spl_20.pdf)
- Jain, S., & Arya, K. (2022). A neoteric strategy of Hill cipher for analysis of degenerate matrices. *Journal of Algebraic Statistics*, 13(1), 194–198. <https://www.publishoa.com/index.php/journal/article/view/74>
- Saeednia, S. (2000). How to make the Hill cipher secure. *Cryptologia*, 24(4), 307–317. <https://doi.org/10.1080/0161-110090896000>
- Santoso, Y. S. (2021). Message security using a combination of Hill cipher and RSA algorithms. *Jurnal Matematika dan Ilmu Pengetahuan Alam LLDikti Wilayah I (JUMPA)*, 1(1), 20–28. <https://doi.org/10.31294/jumpa.v1i1.10417>
- Qowi, Z., & Hudallah, N. (2021). Combining Caesar cipher and Hill cipher in generating encryption key on the Vigenère cipher algorithm. *Journal of Physics: Conference Series*, 1918(4), 042004. <https://doi.org/10.1088/1742-6596/1918/4/042004>