ENCODING AND DECODING OF SECRET MESSAGES USING MATRICES

BY

NIWAGABA JAMES

17/A/BSCED/0167/F

A REPORT BOOK SUBMITTED TO THE FACULTY OF EDUCATION IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR'S DEGREE OF SCIENCE WITH EDUCATION AT KABALE UNIVERSITY

MARCH, 2020

DECLARATION:

I do hereby declare that this Project report is original and has not been published and/or submitted for any other Bachelor award to other University before.

Signature:................

NIWAGABA JAMES Date: 01/02/2021

17/A/BSCED/0167/F

ς

APPROVAL:

This Report has been submitted for review with my approval as supervisor:

Signature:.~,

Date: 01/02/2021

MR. KATENDE RONALD

Academic Supervisor.

DEDICATION:

I dedicate this project report to my beloved family , my friends and my Class mates. Supervisor: MR KATENDE RONALD Thank you very much for all the support you rendered to me.

ACKNOWLEDGEMENT:

I am gratefully thank God who has enabled me to complete this project report successfully, my family for the financial support rendered to me and for the support they are still rendering to me.

I also appreciate my friends for the guidance and support they gave to me. Finally, I thank my Supervisor Mr.Katende Ronald for the advice and guidance given to me regarding my project.

ABSTRACT

This project examines the encoding and decoding of very sensitive information using matrices. In order to unfold the history of encoding and decoding, the influence of matrices in the mathematical **world** is spread wide because it provides an important base to many of the principles and practices. It is important that we first determine what matrices is. Due to the great need of security for passing sensitive information from one person to another or from one organization to another through electronic technology, there is need for cryptography as a solution to this problem. Matrix analysis of one sort or another has for the past century been used in a variety of disciplines to summarize complex aspects of knowledge generation and to provide an eagle's eye perspective of them. It is hoped that this activity of encoding and decoding messages not only offers teachers write great opportunities to either introduce or consolidate certain mathematical concepts and algorithms but also to convince their students that mathematics plays an important role in various walks of life and hence is a useful and meaningful field of study.

TABLE OF CONTENTS

CHAPTER ONE:

GENERAL INTRODUCTION

1.0 Back ground of the study.

In order to unfold the history of encoding and decoding, the influence of matrices in the mathematical world is spread wide because it provides an important base to many of the principles and practices. It is important that we first determine what matrices is. As such, this definition is not a complete and comprehensive answer, but rather a broad definition loosely wrapping itself around the subject (Jeff, 2012).

"Matrix" is the Latin word for womb, and it retains that sense in English. It can also mean more generally any place in which something is formed or produced.

The origin of mathematical matrices lies with the study of systems of simultaneous linear equations. An important Chinese text from between 300Bc and 200Ad, Nine chapters of the mathematical art, gives the first known example of the use of matrix method to solve simultaneous equations (Laura, 2012)

In the treatises 7th chapter "too much and not enough", the concept of a determinant first appears, nearly two milknna before it's supposed invention by the Japanese mathematician SEKI KOWA in 1683 or his German contemporary GOTTFRIED LEIBNIZ (who is also credited with the invention of differential calculus, separately from but simultaneously with ISAAC NEWTON).

More use of matrix-like arrangements of numbers appears in which a method is given for solving simultaneous equations using accounting board that is mathematically identical to the modern matrix method of solution outlined by cash Friedrich Gauss(1777-1855) also known as Gaussian Elimination (vitull Marie2012).

This project seeks to give an overview of the history of matrices and their practical applications touching on the various topics used in concordance with it.

Around 4000 years ago, the people of Babylon knew how to solve a simple 2x2 system of linear equations with two unknowns. Around 200Bc, the Chinese published that "Nine chapters of the mathematical art" , they displayed the ability to solve a 33 system of equations (perotti). The power and progress in matrices and their applications didn't come to fruition until the late 17th century.

The emergence of the subject came from determinants, values connected to a square matrix, studied by the founder of calculus, Leibniz, In the late 17th century, Lagrange came out with his work regarding Lagrange multipliers, away to characterize the maxima and minima multivariate functions Darkwing) more than 50 years later, Cramer presented his ideas of solving systems of linear equations based on determinants more than 50 years after Leibniz (Darkwing).

Interestingly enough, Cramer provided no proof for solving nn system. As mentioned before, Gauss work dealt much with solving linear equations themselves initially, but didn't have as much to do with matrices. In order for matrix algebra to develop, a process was necessary. Also vital to this process was a definition of matrix multiplication and the facts involving it.

The introduction of matrix notation and the invention of the word matrix were motivated by attempts **to** develop the right algebraic language for studying determinants. In1848 JJ.Sylvester introduced the **term** "matrix" the Latin word for womb as a name for an array of numbers. He usewomb because linear algebra has became more relevant since the emergence of calculus even though it's foundational equation of ax+b=0 dates back century.

Euler brought to light the idea that a system of equations doesn't necessarily have a solution. He recognized the need for conditions to be placed upon unknown variables in order to find a solution. The initial work up until this period mainly dealt with the concept of unique solutions and square matrices where the number of equations matched the number of unknowns. With the turn into the 19th century Gauss introduced a procedure to be used for solving a system of linear equations. His work dealt mainly with linear equations and had yet to bring in the idea of matrices or their notations. His effort dealt with equations of differing numbers and variables as well as the traditional pre-19th century works of Euler, Leibniz and Cramer, Gauss 'work is now summed up in the term Gaussian Elimination. This method uses the concepts of combining, swapping or multiplying rows with each other in order to eliminate variables from certain equations. After variables are determined, the student is then to use back substitution to help in finding the remaining unknown variables.

He viewed a matrix as a generator of determinants (Trucker, 1993).The other part, matrix multiplication or matrix algebra came from the work of Arthur Cayley in 1855.Cayley's defined matrix multiplication as the matrix of coefficients for the composite transformation T2Tl is the product of matrix for T2 times the matrix for Tl (Tucker 1993). His work dealing with matrix multiplication culminated in theorem, the Cayley-Hamilton Theorem simply stated a square matrix satisfies matrices at the end of the 19th century were heavily connected with physical issues and for mathematicians, more attention was given to vectors as they proved to be basic mathematical elements. With the advancement of technology using the methods of Cayley, Gauss ,Leibniz, Euler and others, determinants and linear algebra moved forward more quickly and more effective. Regardless of the technology through Gaussian Elimination still proves to be the best way known to solve a system of linear equations (Trucker, 1993).

The influence of matrices and their applications in the mathematical world is spread wide because it provides an important base to many of the principles and practices. Some of the things matrices is used for are to solve systems of linear fonnat, to find least square best fit lines to predict future outcomes or find the trends, to encode and decode messages. Other more broad topics that it is used for are to solve questions of energy in quantum mechanics. It is also used to create simple every day household games like Sudoku, it is because of these practical applications that matrices has spread so far and advanced. The key, however, is to understand that the history of linear algebra. Although linear algebra is a fairly new subject when compared to other mathematical practices, it's uses are wide spread. With the effort of calculus savvy Leibniz the concept of using systems of linear equations to solve unknowns was formulated. Other efforts from scholars like Cayley, Euler, Sylvester, and others changed matrices into the use of linear algebra to represent them. Gauss brought this theory to solve systems of equations proving to be the most effective basis for solving unknowns. Technology continues to push the use further and further but the history of matrices and their applications continues to provide the foundation. Even though every few years companies update their text books, the fundamentals stay the same (Laura, 2012).

12 Statement of the problem.

There is a problem of using video cipher to encrypt data as there is shortage of privacy and security when passing sensitive information from one person to another or from one organization to another through electronic technology. Thus there is a need for cryptography as a solution to this problem. In this project, matrix inversion is used to encrypt and decrypt data to solve the stated problem.

Objective **of the study.**

To encode and decode data/ information using matrices.

1.4 Significance of the study

The **study** shows that matrix is an indispensable in the application of mathematics to solving scientific problems. The significant of this study varies based on the point of view, it is being looked from. The use of matrix in encoding and decoding information will be of great significance to both individuals, government and any researchers as it will help to keep some information privately.

1.5 SCOPE OF THE STUDY.

1.5.1 Scope content.

The project is intended to cover matrix inversion in encrypting and decrypting information privately.

1.5.2 Time scope.

This project is expected to be completed within one year (2019-2020).

1.6 Limitation of the study.

The project is limited in application of matrices to encode and decode information.

1.7 Definition of terms used in matrices.

Matrix: A matrix is a rectangular array of elements consisting of m rows and n columns. or Matrix is a collection of numbers arranged into affixed number of rows and columns.

Square matrix: A matrix involving the same number of rows and columns is called a square matrix, and the number of rows is called its order. The diagonal contained the elements al 1 ,a22 ....ann of a square matrix of order n. These elements al 1, a22, ann are called the principal diagonal.

Equality of matrix : Two or more matrix of the same order are said to be equal if and only if their corresponding entries are equal. Thus, A=B implies a,=b for all i,j €N.

Triangular matrix: This is a square matrix in which the diagonal is zero. 4

Operations of matrix: The arithmetic operation of matrices is like the arithmetic of numbers, **except** that matrices do not necessarily commute under multiplication and matrices need not have multiplicative inverse.

A unit matrix: A unit matrix is an integer matrix consisting of all ls.

A diagonal matrix: A diagonal matrix is a matrix in which entries outside the main diagonal are all zero.

An elementary matrix is a matrix which differs from identity matrix by one single elementary row operation.

Scalar matrix is a diagonal matrix whose diagonal elements are equal. The scalar matrix I"= (d) where d,=0 and d,=lfor i is not equal to j is called the n n identity matrix.

Argumented matrix is a matrix obtained by appending the columns of two given matrices usually or the purpose of performing the same elementary row operations on each of the given Matrices.

Trace of matrix is the sum of the elements on the main diagonal.

Transpose of matrix is a new matrix whose rows are the columns of the original.

Echelon form of matrix is a matrix fulfilling certain characteristics.

Symmetric; A Matrix A is said to be symmetric if A=AT, that is a_ii = cl-ii for all 1j=l,2, ... n .However, if AT=-A, then the matrix A is called skewed symmetric which implies a _ir{-a} _ij for all ij=1,2, ...n,so in particular all the diagonal elements a -ii are zero.

Addition and subtraction of matrices.

Addition of matrix :if A=[a]m n and B=[b]m n ,then A+B=[a#+by]mn.

For all ij €N. Addition is always commutative and associative.

Subtraction of matrix: Let matrix A be the minued and B be the subtrahend.

Then A-B=A+(-l)B .In other words, to subtract a matrix ,change the sign of the subtrahend (multiplying by-1) and add .For all i,j €N. The number being subtracted is called the subtrahend and the number being subtracted from is called the minued.

The two matrices can be added or subtracted if and only if they have the same dimensions. To add or subtract two matrices of the same dimensions, we add or subtract the corresponding entries. More fonnally if A and B are mn matrices, then A+B and A-B are mn matrices whose entries are given by;

(A+B)=A+B ij" entry of the sum = sum of the ij" entries ,and (A-B)= A#-By ijth entry of the difference = difference of the ij" entries.

Properties of matrix addition.

For mn matrices A, B, and C, the following properties hold;

- A+B=B+A [commutative law for addition].
- A+(B+C) = (A+B)+C [Associative law for addition].
- Closure property: A+B is again an mn Matrix.
- Additive identity: The mn matrix O consisting of all zeros has the property that A+O=A.
- Additive inverse: The m*n matrix (-A) has the property that A+(-A)=0.

Scala r multiplication.

The product of a scalar a times a matrix A, denoted by a A ,is defined to be the matrix obtained by multiplying each entry of A by a .That is[aA]=a[A] for each i and j.

Properties of scalar multiplication.

For mn matrices A and B and for scalars a and B, the following properties hold; ❖

Closure property: aA is again an mn matrix.

- Associative property: [a~]A= a[BA].
- Distributive property: a[A+B]=aA+aB, scalar multiplication is distributed over matrix addition.
- Identity property: IA=A,The number I is an identity element under scalar multiplication.
- Distributive property: [a+B]A= aA+BA, scalar multiplication is distributed over matrix addition.

A matrix A can be added to itself because the expressionA+A is the sum of two matrices that have the same dimensions .When we compute A+A ,we end up doubling every entry in A, so we can think of the expression 2A is telling us to multiply every element in A by 2.

Scalar multiplication: A scalar is a real number. Scalar multiplication is the process of multiplying a scalar by a matrix.

Matrix multiplication.

Let A be a mp matrix and B be a pn matrix, The product AB is a mn matrix where each element is obtained by multiplying the i"" rows and j" column of the product matrix AB .The basic condition for the product of two matrices is that the number of column in matrix A must be equal to the number of row in matrix B.

Properties of matrix multiplication.

For mn matrices A, B, and C, the following properties hold for if 0 is a zero matrix and I is an identity.

- A(BC]=(AB]C (Associative law for multiplication).
- A(B+C]=AB+ AC (Distributive law/Left hand).
- 0A=A0=0.Multiplication by zero matrix.
- AI=IA= A. Multiplicative identity law.

Elementary Row operation.

Elementary matrix operation play an important role in many matrix algebra applications, such as finding the inverse of a matrix and solving simultaneous linear equations.

Any elementary row operation on an integer valued matrix p is defined to be any of the following;

- Interchange two rows.
- Multiply arrow by a non zero integer constant C.
- Add an integer multiple of a row to another a row.

Permutation matrix

A permutation matrix is a matrix obtained from an identity matrix by pennuting the rows of the matrix.

Determinant of a matrix

Detenninants of a square matrix is nothing but the volume of the (higher dimensional) parallelepiped spanned by the vectors represented by the columns or rows of matrix. If A is a square matrix, we associate with it a number denoted by /A] or A. The number of A or /A] is called the determinant of A of order n, written as <let (A). Matrix detenninant for matrix of order 3 and above is obtained by a process called expansion by cofactor.

Minor .The minor M _ij of a_ij is defined as detenninant of the sub matrix obtained from **matrix** A by deleting row i and column j.

Cofactor .The cofactor A_ of A_ is defined as A_=(-1)" M_; where M_ is the minor i.e. the detenninant of the sub matrix obtained by deleting row i and column j.

ς

CHAPTER TWO:

LITERATURE REVIEW.

2.0 **Introduction.**

Marx analysis of one sort or another has for the past century been used in a variety of disciplines to s narize complex aspects of knowledge generation and to provide an eagle's eye perspective of them. :::cz:iples are formal probability theory (Popper, 1959), Linguistic (Chomsky and Ittalle, 1968; Quirk et ii1974, Chen and Wang 1975, Lass 1984). Psychology (Fox, et al., 2001) and in communication science. -::e :ocus of the article, the Matrix method of literature review was popularized as a research tool in the health sciences by Garrard 1999, Later reprinted as Garrard 2004. We have adapted Garrard's method me what to extent it to other disciplines and to make it more flexible from an epistemological point of mew

~ matrix method of literary review protects the reviewer against ignorant assumptions about the ±search theme at a stage that he/she is the most vulnerable due to lack of knowledge about the topic investigation. This of course relates to the conceptual domain of knowledge known as under epistemology.

CHAPTER THREE:

METHODOLOGY.

Matrix inversiQD

Now that we have discussed matrix addition, subtraction and multiplication, you may well be wondering about matrix division. In the realm of real numbers, division can be thought of as a

fonn of multiplication. Dividing 3 by 7 is the same as multiplying 3 by·\ the inverse of 7. In 7

symbols 3:7=34or 37-1 7

In order to imitate division of real numbers in the realm of matrices, we need to discuss the multiplicative inverse, A' of matrix A.

Note; Because multiplication of real numbers is commutative for example!. as either 3 x7-[1] or?-[1] x3 7

In the realm of matrices, multiplication is not commutative so from now on we shall never talk about "division" of matrices (by "" should we mean A'B or BA' ?).

Before we try to find the inverse of a matrix, we must first know exactly what we mean by the inverse. Recall that the inverse of a number a is the number often written a',with the property that a' a=aa'=l.for example

the inverse of 76 is the number 76-L [1], because 76 ($_x 76=76x,-)=I. This is the number calculated by n-'button found on most calculators. Not all numbers have an inverse.

For example and this is the only example that number 0 has no inverse, because you cannot get 1 by multiplying 0 by any thing. The inverse of a matrix is defined similarly.

To make life easier, we shalt restrict attention to square matrices, matrices that have that same number of rows as columns.

Inverse of a matrix; The inverse of an nn matrix A is that nxn Matrix A' which when multiplied by A on either side, yields the n n identity matrix I

thus AA"=A'A=1.

If A has an inverse, it is said to be invertible otherwise, it is said to be singular. ⊄ The inverse'e of the lxl matrix [3] is[~], because [3] [~]=[1].
3 3

·❖ The inverse of the nn identity matrix I is I itself, because IxI=I, Thus I"[1]=I.

ς The inverse of the 22 matrix

L! _Es[; #le

AA-1=[1 −1 [# -1 _! 2! 0 2

And

A-1A=[1/2 −1/2 −1/2 −1/2][1 −1 1-|% -1 0

Notes;

❖ It is possible to show that if A and B are square matrices with AB= I, then it must also be true that BA=I. In other words , once we have checked that AB= I, we know that B is the inverse of A, The second check, BA= I is unnecessary.

❖ If Bis the inverse of A then we can also say that A is the inverse of B (why?).

• Thus we sometimes refer to such a pair of matrices as an inverse pair of matrices.

CHAPTER FOUR.

4.0 Introduction

This chapter explains how the name Niwagaba James was coded *using* matrices and the *question* ct what is your name?

4.1 ENCODING AND DECODINGDATA

RESULTS;

One of the important applications of inverse of non singular square matrix is in cryptography. Cryptography is an art of communication between two people by keeping the information not known to others. It is based upon two factors namely encryption and decryption.

Encryption is the process of transformation of information (plain fonn) into an unreadable form coded form). On the other hand, Decryption means the transfonnation of the coded message back into original form. Encryption and Decryption require a secret technique which is known only to the sender and the receiver.

This secret is called a key. One way of generating a key is by using a non singular matrix to encrypt a message by the sender. The receiver decodes (decrypts) the message to retrieve the original message by using the inverse of matrix. The matrix used for encryption is called encryption matrix (encoding matrix) and that used for decoding is called decryption matrix (decoding matrix).

We explain the process of encryption and decryption by means of an example.

Suppose that the sender and receiver consider messages in alphabets A to Z only both assign the numbers 1 to 26 to the letters A to Z respectively, and the number 0 and 27 to represent a blank space and ? respectively. In summary consider the following table.

Ee ABC/DE F/GH I]J K L M N O P Q R S T U V W X Y Z ?

f 123 4]56 7/8/9/10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

For simplicity, the sender employs a key as post multiplication by a nonsingular matrix of order 3 of his own choice. The receiver uses post multiplication by the inverse/adjoint of the matrix which has been chosen by the sender.

SENDER'S MESSAGE

Use the encoding matrix

40	-31	23
29	-20	20
44	-19	19
75	-36	15
15	-14	0
80	-18	1

-1 1

-1 0) and Coded row matrix to interpret the message.

0 0

1 0 0

Required by the received to interpret the message.

Step 1: Get the decoding matrix from encoding matrix by finding the cofactor matrix of the encoding matrix and then transpose it to get the adjoint **which** is the same as encoding matrix i.e. Adjoint (A)= (cofactor matrix)' = decoding matrix.

- If a is an x n matrix with n greater than one (n> 1), the minor M_{ij} is the determinate of the (n-1) (n-1) sub matrix of a obtained by deleting the i^{th} row and **j** column of matrix A

- The cofactor A_{ij}, associated with M_{ij} is defined by $A_{ij}= (-1)^{i+j}M_{ij}$ Therefore, let the cofactors of encoding matrix

·$3% **be** in the form $\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$

From $A_{ij} = (-1)^{i+j} M_{ij}$

An=(-1)f' 0 0 c = A-cw %0

$A_{13} = (-1)^4 \begin{vmatrix} 2 & -1 \\ 1 & 0 \end{vmatrix} = 1$ A =(-1)' · [[0

A cw |; }-+ $A_{23} = (-1)^5 \begin{vmatrix} 1 & -1 \\ 1 & 0 \end{vmatrix} = -1$

$A_{31} = (-1)^4 \begin{vmatrix} -1 & 1 \\ -1 & 0 \end{vmatrix} = 1$ $A_{32} = (-1)^5 \begin{vmatrix} 1 & 1 \\ 2 & 0 \end{vmatrix} = 2$

A33 = (-1)6 . |:_- -~L r

·~ erefore Cofactor matrix ~ G -] -D But

o =0i i1)
(

adioint (A) = Cofactor matrix) θ =0~ 21 1) Decoding matrix = ~
(

Thus the decoding matrix = ~

Step 2: multiply the coded row matrix and decoded matrix together to get the decoded row :natrix which contain numerical value

Coded row matrix			Decoding matrix			Decoded row matrix				Alphabet letters		
40	-31	23				23	8	1		*W*	*H*	*A*
29	-20	20		0		20	0	9		*T*		*I*
44	-19	19	G	-1	D =	19	0	25	=	*S*	_	*y*
75	-36	15		-1		15	21	18		0	*U*	*R*
15	-14	0				0	14	1		_	*N*	*A*
50	-18	13				13	5	2		*M*	*E*	?

By organizing the letters of the alphabet, then the RECEIVER can interpret the message as WHAT IS YOUR NAME?

43 FEEDBACK FROM THE RECEIVER

can *also* use the same encoding *matrix*

1	-1	
2	-1	%
1	0	

and coded row matrix =

63	-38	13
29	-15	14
14	-5	5
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
6	-3	1
21	-10	0
42	-18	13

to interpret the message

Required by the SENDER to interpret the message

Set t Finding the decoding matrix.

Ser 2 Finding the decoded row matrix as said before.

Decoding matrix -G 0 -1 -1 »

Coded row matrix			Decoding matrix	Decoded row matrix			Alphabet letters		
63	-38	13		13	25	0	M	y	_
29	-15	14		14	1	1	M	A	M
14	-5	5	G 0 %	5	0	9	E	_	I
56	-33	19		19	14	9	S	N	I
32	-24	23	-	23	1	7	W	A	G
6	-3	1	1	1	2	1	A	B	A
21	-10	0		0	10	1	_	J	A
42	-18	13		13	5	1	M	E	S

ganising the letters of the alphabet, then the SENDER can interpret the feedback as NAME **IS** NIWAGABA JAMES .

CHAPTER FIVE

conclusion

secondary school students often ask their teachers why it is important to learn mathematics, and their achers are usually faced with the challenge of explaining and it's importance and relevance to real life suations to convince them. However, this may not always be easy task.

therefore it is hoped that this activity of encoding and decoding messages not only offers teachers write great opportunities to either introduce or consolidate certain mathematical concepts and algorithms but aaso to convince their students that mathematics plays an important role in various walks of life and hence a useful and meaningful field of study.

REFERENCES:

Darkwing, n.d. *A brief history of linear algebra and matrix theory*.

Fox, RA, McManus, I. & Winder, B. (2001). *British Journal ofEducational Psychology*.

s.1. :s.n.

Jeff, *C. (*2012). *A Brief History of Linear Algebra*, s.l.: University of Utah.

Laura, s. (2012). *Ancient Chinese Mathematics (1600 BC - 600 AD),* s.l.: https://math-physics-biems.wikia.org/wiki/Ancient_Chinese_Mathematics_(1600_BC_-_600_AD).

popper, K. R. (1959). *The Propensity Interpretation of Probability,* s.l.: Oxford University Press. Trucker (1993) .A Brief History of Linear Algebra. *christensen-HistoryLinear Algebra. pdf.*