Parallel Algorithm for Finding Inverse of a Matrix and its Application in Message Sharing (Coding Theory)

Shruti Saraf
SCOPE
VIT University

Swati Dhingra
SCOPE
VIT University

Greetta Pinheiro
SCOPE
VIT University

ABSTRACT
A parallel algorithm for finding the inverse of the matrix using Gauss Jordan method in OpenMP. The Gauss Jordan method has been chosen for this project because it provides a direct method for obtaining inverse matrix and requires approx. 50% fewer operations unlike other methods. Hence forth it is suitable for massive parallelization. Then, authors have analyzed the parallel algorithm for computing the inverse of the matrix and compared it with its perspective sequential algorithm in terms of run time, speed-up and efficiency. Further, the obtained result is used to propose a new method of Message Sharing (called Coding Theory). The proposed method is simple and has a great potential to be applied to other situation where the exchange of messages is done confidentially such as in military operation, banking transactions etc.

General Terms
Matrix Inversion, Security, Digital Image Processing

Keywords
Gauss-Jordan Elimination, LU Decomposition, QR Decomposition, Cholesky decomposition, 3D transformations, OpenMP, Message Sharing

1. INTRODUCTION
Matrix Inversion is an essential step in a wide range of numerical problems- starting with solving linear equations, structural analysis using finite element methods, 3D rendering, digital filtering, image filtering, image processing and constitutes an indispensable component in almost all mathematical/ statistical software suits [9]. Finding the inverse of a square matrix can be done using a variety of methods, including well-known methods such as Gauss Elimination, Gauss- Jordan, LU Decomposition, QR Decomposition and Cholesky Decomposition [10].

One of the applications of Matrix Inversion is Message Passing (Coding Theory). Coding theory is the study of the properties of codes and their fitness for a specific application. Codes are used for data compression, cryptography, error-correction and more recently also for network coding. Coding theory finds its application in exchange of messages in confidential and more secured way. It has wide application in Military operations, Banking Transactions etc. [7],[8].

Since determination of the inverse of non singular matrices of higher order is difficult and this requires higher level algorithms for the use of computers. The most proficient approach to increase efficiency is to adopt parallel principles. A newly developed method that avoids the difficulties in the determination of inverse of a non singular matrix is introduced in this paper. Cryptography which is the branch of Coding Theory is implemented here. The results obtained using this method works very well for the whole range of message exchanging problems and the excellent agreement with the existing one [11].

Keeping in goals of cryptography like Confidentiality, Data integrity, Authentication etc, authors have designed our system in a quite simple manner but off-course not sacrificing with security issues. Also, various cryptographic algorithms developed by various people are not cost effective since those are not designed for small amount of data. Proposed cryptosystem is designed to address this issue so that authors don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. The proposed cryptosystem is capable of encrypting and decrypting messages of any length.

Rest of this paper is organized into 8 sections as follows: In Section 2 briefly describes Cryptography, Section 3 describes Problem Definition, Section 4 outlines Literature Review, Section 5 portrays Algorithm, Section 6 Proposed Methodology, Section 7 describes Results and Discussion and Conclusion is discussed in the last section.

2. OVERVIEW OF CRYTOGRAPHY
In the information age, cryptography has become one of the major methods for protection in all applications [8]. Cryptography allows peoples to carry over the confidence found in the physical world to the electronic world [12]. It permits people to do business electronically without worries of fraud and hypocrisy in the distant past, cryptography was used to assure secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assured integrity of the message and authenticity of the sender [12].

At the point when individuals began working together online and expected to exchange found electronically, the use of cryptography for integrity began to surpass it use for secrecy. A huge number of individuals communicate electronically consistently, whether it is through email, e-trade (business led over the web), ATM machines or mobile phones. The steady increment of data transmitted electronically has lead to an expanded dependence on cryptography and verification. An evident application of cryptography is concerned with keeping communication private. Cryptography mainly consists of encryption and decryption.

Encryption is the transformation of data in to some unreadable form its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended even those who can see the encoded data [12]. Decryption is the reverse of encryption it is the transformation of encoded data back in to some intelligible form. Encryption and decryption require the utilization of some secret information, usually referred to as a key depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the

keys used for encryption and decryption might be distinctive [13]. The above concepts are applied in our paper.

3. PROBLEM DEFINITION

There are two approaches of designing a good parallel algorithm. The first is to start from a good sequential algorithm and build a parallel version out of it. The second approach is to minimize the parallel time allowing an arbitrary number of processors. However, authors have applied the first approach and started from sequential algorithm toward the parallel version using OpenMP. The Gauss Jordan method has been chosen for this project because it provides a direct method for obtaining inverse matrix and requires approx. 50% fewer operations unlike other methods. The above obtained calculations are made use in a newly proposed cryptographic method which can be used in message sharing. This method will provide more security to the messages which are send through an unsecured channel.

4. LITERATURE REVIEW

The analysis on the Gauss elimination and LU decomposition using OpenMP and MPI environments have been carried out. Based on the results of examining various load balancing schemes on both platforms, it shows that in OpenMP, Data can be made available to all processors at all times. But in case of MPI, when authors increase the value of n, the program displays an improvement in performance [1]. The Gauss elimination method without pivoting was introduced to explain the concepts both in OpenMP and MPI where in MPI, communication capabilities between the nodes increases apparently along with the floating point speed [2].Finite algorithms for solving system of linear equations using Gauss elimination method was designed for shared memory, distributed memory and also for their combination. There was still a need for more efficient communication algorithm, which will be adapted to new architecture of parallel computers [3][4].

The inverse and determinant of square matrix was calculated using order expansion and order condensation respectively. If in the process of calculations, the pivot elements steeply tends to zero, then the matrix is singular otherwise the product of all these pivot elements will give the determinant. Both real and complex entries were possible and was accepted by the matrix [5]. The Cholesky decomposition reduced the number of operations by avoiding computation of intermediate results in computing the matrix inversion. Fixed point simulations were used to compare the numerical accuracy of the method. It also eliminated the square root operations [6].

5. ALGORITHM

Algorithm includes two phases - Encoding and Decoding which are described in below sections.

5.1 Encoding Process

1. Represent the text message into a stream of numbers for both the sender and the receiver.

2. Place the numbers obtained in step 1 into a matrix of order m×n where n depends on the size of the message and this may be called as a Message matrix M.

3. Multiply M by the Encryption key matrix E of size n and get the encoded matrix X.

4. Pass the encrypted matrix as a stream to the receiver.

5.2 Decoding Process

1. Take the encrypted stream of numbers as received by the sender and represent it in form of a matrix.
2. Multiply the encoded matrix with the decryption key D which is the inverse of the key used for encryption for message matrix M.
3. Convert this message matrix in to a stream of numbers.
4. Convert this stream of numbers into the text of the original message.

6. PROPOSED METHODOLOGY

The proposed system is an application of the inverse of a square matrix. Here, authors parallelized a sequential algorithm to find the inverse of a square matrix after considering the dependencies. The comparison of both the sequential and parallel algorithm was done. Based on the runtimes, speedup and efficiency of the parallel algorithm showed better performance than its underlying sequential algorithm.

The new cryptographic system was developed for secure message sharing in an unsecured channel. This cryptographic system uses inverse of a square matrix both sequential and parallel. Description of the process can be understood by referring to Figure 1 which gives the overview of the system. The proposed system is a modification of symmetric key cryptosystem also referred to as conventional cryptography or secret key cryptography. In secret key cryptography, a single key is used for both the process i.e. encryption and decryption. The sender uses a key to encrypt the plaintext and send the encrypted message to the receiver.

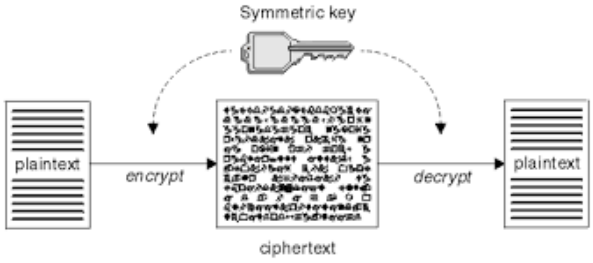

Fig 1: Symmetric Key Cryptography

The receiver applies the same key which was used for encryption or a key which is very similar to it in order to decrypt the message to get the plaintext. In our proposed cryptographic system, same key is used for encryption and decryption but key used in decryption is the inverse of the key used in encryption. In this type of cryptography, it is clear that the key will be known to the sender and the receiver both.

Figure 2 shows a diagrammatic view of the components of the proposed system. The encryption algorithm uses a key matrix which is generated by the system. It is a secret key (K). The user entered message is converted into a matrix with its corresponding numbers which is predefined (M). The key (K) is multiplied with the message matrix (M). In order to improve the performance of the encryption authors have parallelized the multiplication. This result after the multiplication will be the cipher text (KM) which is sent to the receiver.

Cipher Text = KM

At the receiver side, the decryption algorithm uses the cipher text (KM) which is received from the sender along with the inverse of the secret key (K^{-1}) which is calculated using the inverse algorithm (using Gauss Jordan). The obtained cipher text (KM) is multiplied with the inverse of the matrix (K^{-1}). The secret key (K) and the inverse of the secret key (K^{-1}) cancels each other. Then the decrypted message (M) can be retrieved as.

Message = $(KM)*(K^{-1}) = M$

In order to compare the efficiency of the parallel and sequential versions of the matrix inversion algorithm, authors have used both of the algorithms in our cryptographic application. The parallel version of the inverse of matrix has better performance in contrast to sequential version. Due to the parallelization of the inverse of the matrix and also the multiplication operations in the calculation, the system can encrypt and decrypt the messages faster than the sequential method. This will help to save time if the message length is more. The system is capable of encrypting and decrypting messages of any length.

7. RESULTS AND DISCUSSION

Consider a user who wants to send "aaa" to other place, and then he will input "aaa" as the plain text message. The system will first convert the message in a matrix filling blank space and extra elements as @, as shown below –

a	a	a
@	@	@
@	@	@

Next, the matrix will be converted it an equivalent number form –

$$P = \begin{matrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

If the key for the encryption is –

$$K = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

Then using the equation, C=PK we get

$$C = \begin{matrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

This cipher text is passed to the receiver

For decryption, the received cipher text is made into matrix form –

$$C = \begin{matrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

The key which was used for encryption was given as input to the inverse program and the inverse matrix is been used as the key for decryption.

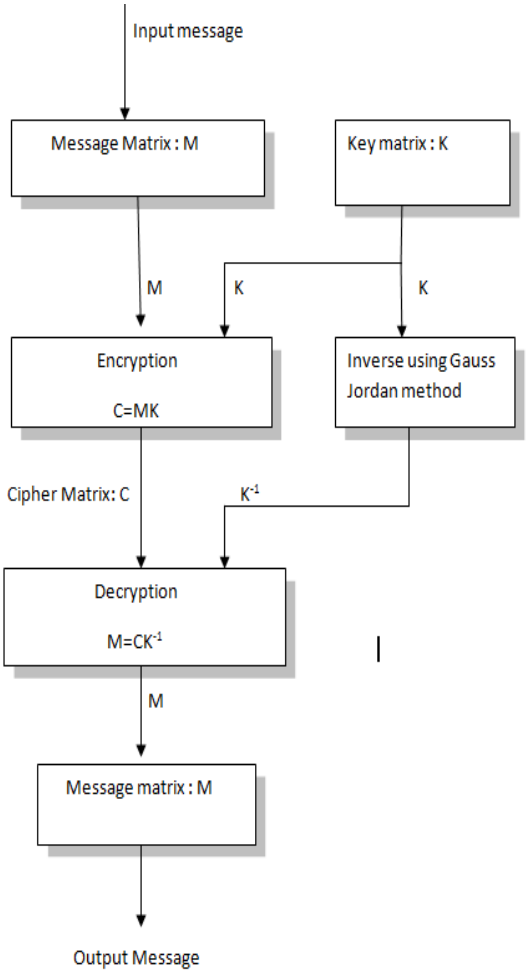

Fig 2: Algorithm Execution

The key used for decryption is –

$$K^{-1} = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

Upon using the equation $P=CK^{-1}$ we get,

$$P = \begin{matrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

The decrypted plain text in form of matrix is -

a	a	a
@	@	@
@	@	@

Finally the decrypted plain text is "aaa".

For the message and key matrices of size 10x10,20x20,30x30 Serial and Parallel Encryption and Decryption times are tabulated in Table 1 and Table 2 respectively with their corresponding graphs in Figure 3 and Figure 4.

Table 1. Serial Encryption-Decryption Time

Matrix size	Input size (Message Length)	Serial Encryption	Serial Decryption	Total Time
10	100	0.011719	0.003906	0.015625
20	100	0.025257	0.000395	0.025652
30	100	0.030440	0.000614	0.031054

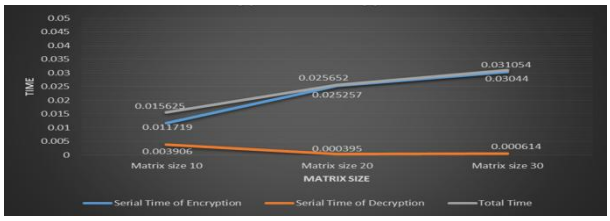

Fig 3: Serial Encryption Time-Decryption Time

Table 2. Parallel Encryption-Decryption Time

Matrix size	Input size (Message Length)	Parallel Encryption	Parallel Decryption	Total Time
10	100	0.000254	0.000021	0.000275
20	100	0.000299	0.000004	0.000303
30	100	0.000395	0.000008	0.000403

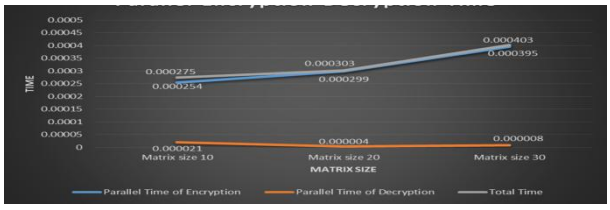

Fig 4: Parallel Encryption Time-Decryption Time

Performance of a system can be measured in terms of speedup and efficiency. Speedup is the measure of how much faster the computation executes versus the best serial code. It can be computed as given in equation 1.

$$Speed\ up = \frac{Serial\ \ Time}{Parallel\ \ Time} \quad (1)$$

Efficiency is defined in terms of speedup per processor. It the measure of how effectively computation resources (threads) are kept busy. It can be computed as in equation 2.

$$Efficiency = \frac{Speed\ \ up}{No.of\ Threads} \quad (2)$$

Speedup and efficiency are calculated from the values of table 1 and table 2. Since authors have used Intel quad core i3 processor , hence number of threads is equal to number of quad i.e. 4. Speedup and Efficiency computed are tabulated in Table 3.

Table 3. Speedup and Efficiency

Matrix Size	Speedup	Efficiency
10	56.81	14.2025
20	84.66	21.165
30	77.05	19.26

It is observed that parallel cryptography technique showed better performance than the sequential algorithm in terms of speedup. Also, the proposed cryptography system provides better security for message sharing in unsecured channel. Since the secret key is generated automatically, brute force attach can be minimized.

8. CONCLUSION

The proposed cryptographic system is capable of providing better security to the messages which is shared using an unsecured channel. The encryption and decryption techniques used in the proposed algorithm is a new technique which is formulated using the inverse of a square matrix. The encryption requires a key matrix, which is fixed by the programmer and so it has a secret behavior. The inverse of this key is calculated using Gauss- Jordan method and is used in the decryption. With the use of parallel inverse algorithm of the matrix, the system can decrypt the message much faster than its sequential algorithm. The efficiency of the system is increased in terms of runtime with the use of parallel algorithms. The security is also increased due to the usage of the inverse of the matrix in the cryptography technique. Thus the proposed system finds application in different fields like military, surveillance and banking.

9. ACKNOWLEDGMENT

The authors are pleased to thank Mrs. J Saira Banu on her valuable comments which helped us in improving our research clarity. Authors also extend thanks to their friends.

10. REFERENCES

[1] S.F.McGinn, R.E.Shaw, “Parallel Gaussian Elimination Using OpenMP and MPI”,Proceedings of the 16th Annual International Symposium on High Performance Computing Systems and Applications (HPCS’02) 0-7695-1626-2/02,2002

[2] Karen H. Warren, Eugune D. Brooks III, “Gauss Elimination: A case study on Parallel machines”, Massive parallel computing initiative, Lawrence Livermore National Laboratory, CA 94550

[3] Martin Hudik,Michal Hodon,“Modelling, optimization and performance prediction of parallel algorithms”, European Regional Development Fund and the Slovak state budget for the project ”Research Centre of University of Zilina”, ITMS 26220220183

[4] MartinHudik, Michal Hodon,“Performance optimization of parallel algorithm”,Journal Of Communications And Networks, Vol. 16, No. 4, August 2014

[5] “Inverse and determinant of a square matrix by order expansion and condesation”

[6] Aravindh Krishnamoorthy, Deepak Menon, “Matrix inversion using cholesky decomposition”, IEEE-SPA 2013 September 26-28, Poznan, Poland, 2013

[7] "Applications of Matrices and Determinants", http://www. richland.edu / james /lecture /.../matrices/applications.html. 2015

[8] "Matrices- Applications to Crytography", http://aix1.uottawa.ca/~jkhoury/cryptography.htm

[9] Girish Sharma , Abhishek Agarwala , Baidurya Bhattacharya, "A fast parallel Gauss Jordan algorithm for matrix inversion using CUDA", Computers and Structures 128 (2013) 31–37

[10] Sami Almalki, Saeed Alzahrani, Abdullatif Alabdullatif, " New parallel algorithms for finding determinants of NxN matrices", Proceedings of the Computer and Information Technology (WCCIT) IEEE, 2013

[11] Balakrishnan Vellaikannan, Dr. V. Mohan, "A Novel Method for Coding Theory With the Help of a Class of Matrices", World Applied Programming, Vol (1), No (5), December 2011. 339-345

[12] Sadiq Shehu, "Application of Matrices to Cryptography", http://www.academia.edu/8377683/APPLICATION_OF_CRYPTOGRAPHY_IN_MATRICE

[13] B.Vellaikannan,Dr.V.Mohan,V.Gnanaraj, " A NOTE ON THE APPLICATION OF QUADRATIC FORMS IN CODING THEORY WITH A NOTE ON SECURITY", Int. J. Comp.Tech. Appl,Vol 1 (1), 78-87