Text Encryption with Singular Values Decomposition Aided- level one

Mohammed Abdul-Hameed

Mathematical Department/College of Basic Education/University of Kufa

Najaf, Iraq

E-mail: mohammeda.alkufi@uokufa.edu.iq

ABSTRACT

This paper we will address the encryption process text is generally through a number of processes of dispersion of the later values in a matrix is A through remittances linear in addition to the use of svd enters, including one key, where work will begin the application process distracting initial. In a compound to generate new matrices B1 and B2 of the original text matrix and which enters the key .The second phase of the dispersion is using SVD on the last matrices and switch S matrix among the two spectral for the new matrices C1 and C2 which represents putting as correlative \( F = [C1 \ C2] \) the matrix of the initial of the encoded text.

For purpose of ascertaining the accuracy of the work we calculated the matrix of absolute value of the difference between the matrix of numbers for original text characters lettering before encryption and matrix of numbers for text characters after decryption to show us zero matrix, as well as the calculation of the average values of this matrix was zero.

KEYWORDS: Text, Encryption text, SVD,M.K. Text Cipher

1 INTRODUCTION

The issue of maintaining the security and privacy of databases (Database Security And Privacy) from the important problems in database applications through networks of various communication against spambots activity of unauthorized (Unauthorized Activity) Access to the data or manipulate it and the provision of a particular method to register all activity spambots while retaining full registrations of all the processes of update the data that take place on a databases away from the hands of the beneficiaries (Users) helps the Database Administrator to improving the security situation and the privacy of her future it must include the programs used in dealing with databases emphasizing the security and confidentiality of the data and to prevent use of improper to grant the specific Permissions and by nature of and quality of the beneficiary with continuous monitoring of the activities of the use of the system

Provides most of current applications, databases and many of the means of protection for databases such as (passwords and data encryption).

Passwords:

All database applications provide a way to add passwords, in addition to the possibility of the beneficiary providing programs his own to use passwords away from passwords provided by database applications. And to choose passwords must follow the following procedures:-
Stay away from the usual choice of password, for example, the person's name, date of birth, family name, name of the director of work ... etc. (where this method provides ease of guessing.

Passwords are chosen as a combination of letters, numbers and special symbols provided by the operating systems in the calculator shows the following example, the number of letters, numbers and special symbols that can be used in the selection of passwords (depending on what the availability the English language only)

The numbers = 11.
Number of characters = 52 (lower/upper case).
Special symbols provided by the keyboard =33.

Will be the total =95. letter, number and special code is added to all the shapes of the letters provided by any language except English to become field choice is very wide.

Preferably that the length of the password at least 11 (characters, number, or special symbol) and the following table shows the time required to guess the password:

<table>
<thead>
<tr>
<th>Number of characters used</th>
<th>Number of the attempts</th>
<th>The time required</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>81450625</td>
<td>71.6464 hour</td>
</tr>
<tr>
<td>6</td>
<td>7.3509e+11</td>
<td>116.5481 year</td>
</tr>
<tr>
<td>8</td>
<td>6.6342e+15</td>
<td>631110 year</td>
</tr>
<tr>
<td>10</td>
<td>5.9874e+19</td>
<td>1898600000 year</td>
</tr>
</tbody>
</table>

Possibility of choosing more than a password to the important beneficiaries for example a database manager.

Importance of the choice of passwords that its validity associated with time on the day.

Data encryption:-

Procedures for data encryption Includes a comprehensive encryption for data or partial encryption where is encrypted portion of the data so that no allow hackers through different computer networks. Possibility of knowing the nature of the data by withholding this data and data structures used them. An example of this encryption all the major and minor keys in tables of data structures used. The process of encryption using an encryption key it is possible to use more than one key to encrypt the data according to its importance. The controls of select the key subject to the same controls for selecting the password follow through regimes implemented in any institution after the transformation of the systems implemented on one computer (only one beneficiaries) to Systems adopted the principle of (the server and the beneficiary) with retaining structures, programs and data (Previous unchanged), popped the following security problems.

Each beneficiary with in the network can to review and update all system tables without notation what he had done and what is the nature of the beneficiary changed information (means that there is an opportunity to manipulate data without leaving a trace of it).

Can use the one computer linked to the network to change all this data at any time when the server in the case on.
So it rolls it is necessary that the focus is on the issue of the security of the data, documents and information and keep abreast of developments in this field, because of weakness in this subject will make the country unprotected and available to breakthrough and Information pirates, which would cause a loss of Informatics lead to a negative impact on the economic side as shown by the histogram following which shows the amount of the economic impact on one of the joints to work in a state where only the health aspect illustrated how important information security at present where all the nations of the world are subject to the effects of globalization and the development of modern scientific

Figure 1. Economic impact of data breach incidents experienced over the three years (2010, 2011, 2012)

2 SINGULAR VALUE DECOMPOSITION (SVD)

Let $A$ be an $m \times n$ real matrix. Then there exist orthogonal matrices $U$ of size $m \times m$ and $V$ of size $n \times n$ such that

$$A = U S V^T$$

Where $S$ is an $m \times n$ matrix with nondiagonal entries all zero and:

$$s_{11} \geq s_{22} \geq \cdots \geq s_{pp} \geq 0$$

where $p = \min\{m, n\}$

Note:
The diagonal entries of $S$ are called the singular values of $A$. The columns of $U$ are called the left singular vectors of $A$. The columns of $V$ are called the right singular vectors of $A$.

$$A = \operatorname{col}_1(U)s_{11} \operatorname{col}_1(V)^T + \operatorname{col}_2(U)s_{22} \operatorname{col}_2(V)^T + \cdots + \operatorname{col}_p(U)s_{pp} \operatorname{col}_p(V)^T \cdots (6)$$

Let $V(A^T A)V^T = D$

$D$ is diagonal matrix whose diagonal entries $\lambda_1, \lambda_2, ..., \lambda_n$ are the eigenvalues of $A^T A$.

$v_j$ denote column $j$ of $V$. 
Not: each eigenvalue of $A^TA$ is nonnegative.
let the eigenvalues of $A^TA$ is $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$
Define $s_{jj} = \sqrt{\lambda_j}$
$V$ is orthonormal matrix $\Rightarrow$ each of it’s columns is a unit vector.
$\Rightarrow \|v_j\| = 1$
Thus the singular values of $A$ are the square roots of the eigenvalues of $A^TA$.

The matrix $U$ is to be orthogonal, it’s columns must be an orthonormal set. Hence they are linearly independent $m \times 1$ vectors.

$$
\begin{bmatrix}
s_{11} & 0 & \cdots & 0 \\
0 & s_{22} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & s_{pp} \\
0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 \\
\end{bmatrix}
\begin{bmatrix}
u_1 \\
u_2 \\
\vdots \\
u_m \\
\end{bmatrix} = \begin{bmatrix}
s_{11} & 0 & \cdots & 0 \\
0 & s_{22} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & s_{pp} \\
0 & 0 & \cdots & 0 \\
\end{bmatrix}
\begin{bmatrix}
u_1 \\
u_2 \\
\vdots \\
u_n \\
\end{bmatrix}
\Rightarrow Av_j = s_{jj}u_j \Rightarrow u_j = \frac{1}{s_{jj}}Av_j
$$

3 METHODOLOGY

3.1 Encryption

The full algorithm to encrypt the text in general:
Beginning we define one key to entered within the matrix of text encryption phases which real but not equal zero.

Identification the numbers corresponding to the letters of the text you want encrypted, including commas and point the bow and all that falls within the composition of the text numbers which is are stored in computer memory. Generally can specify a special table for the numbering of the characters and the signals which are used in the writing of the text.

Using the method of (DATA CUBE) we transform the numbers of text components to three-dimensional matrix. Let this matrix $A$.

In this step, we will use the method of distracting the matrix numbers to create a matrix $B_1$ and $B_2$
$B_1=$Key$\ast A$, $B_2=$-Key$\ast A$

Apply SVD Distracting the numbers:

$[UB_1,SB_1,VB_1]=$SVD(B1) $[UB_2,SB_2,VB_2]=$SVD(B2)

$C_1=UB_1\star SB_2\star [[VB_1]]^T$, $C_2=UB_2\star SB_1\star [[VB_2]]^T$

$F=[C_1 \ C_2]$
Text Cipher = F

The full paper has to be submitted electronically via the website of the conference) by

Paper number (in the format "XXX") is assigned to each abstract after it was submitted through our OpenConf system and authors are kindly asked to place this paper number to the correct positions in the header and footer before submitting the final version.

3.2 Decryption

_text decryption:_
The full algorithm to decrypt of the text.

Now, with phases of decode matrix of text.

We have matrix is encrypted M. K. Text Cipher1 = F

1- Divide the matrix \( F_{new} \) to restore matrices \( C1_{new} \) and \( C2_{new} \)
2- Reflect the impact of (SVD Distracting the numbers) that is in step 5 of the encryption process to restore matrices \( B1_{new} \) and \( B2_{new} \).

\[
[UC1_{new}, SC1_{new}, VC1_{new}] = \text{SVD}(C1_{new}) \quad [UC2_{new}, SC2_{new}, VC2_{new}] = \text{SVD}(C2_{new})
\]

\[
B1_{new} = UC1_{new} * SC2_{new} * VC1_{new}^T, B2_{new} = UC2_{new} * SC1_{new} * VC2_{new}^T
\]

3- \( A_{new} = \frac{B1_{new}}{key} \)

The last matrix \( A_{new} \) represent the numerical values of the letters of the cipher text after decryption they include the error increase or decrease of less than 0.5 which is cannot represent the numerical values for letters. So we approximation of each value to the nearest integer, as in below:

\[
45.456 \approx 45, \quad 36.743 \approx 37 \ldots etc
\]

Bringing we produces matrix of numerical values for letters of cipher text identical to the original matrix and without any error.

From the last matrix we recover the letters and symbols corresponding to the numerical values of it to show the same original text and without any error.

4 THE RESULT

4.1
The text Before encryption:-

This paper we will address the encryption process text is generally through a number of processes of dispersion of the later values in a matrix is A through remittances linear in addition to the use of svd enters, including three keys sequentially, where work will begin the application of the closed set [0,1] while retaining the largest value and the smallest value... In the matrix FF within the last matrix to ensure the possibility of return versa in the decryption phase in a way that we called (MK press numbers) The final matrix resulting matrix is the final encrypted text that we call (M.K. Text Cipher1).

4.2

The numbers corresponding to the components of The text

The final matrix resulting matrix is the final encrypted text that we call (M.K. Text Cipher1).
Matrix of the encryption of numbers for the text and it consist of 4000 element:
<table>
<thead>
<tr>
<th></th>
<th>f(:,:,2)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>1.0440</td>
<td>0.0910</td>
<td>1.0260</td>
<td>1.0260</td>
<td>0.0910</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>1.0440</td>
<td>0.0910</td>
<td>1.0440</td>
<td>1.0440</td>
<td>0.0910</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>1.0530</td>
<td>0.9360</td>
<td>0.9360</td>
<td>1.0530</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.9450</td>
<td>0.6300</td>
<td>0.9360</td>
<td>0.9360</td>
<td>0.6300</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2920</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9450</td>
<td>0.6300</td>
<td>0.9360</td>
<td>0.9360</td>
<td>0.6300</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2920</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9450</td>
<td>0.6300</td>
<td>0.9360</td>
<td>0.9360</td>
<td>0.6300</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9450</td>
<td>0.6300</td>
<td>0.9360</td>
<td>0.9360</td>
<td>0.6300</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9450</td>
<td>0.6300</td>
<td>0.9360</td>
<td>0.9360</td>
<td>0.6300</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9450</td>
<td>0.6300</td>
<td>0.9360</td>
<td>0.9360</td>
<td>0.6300</td>
<td>0.9900</td>
<td>0.9900</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
<tr>
<td>0.9900</td>
<td>0.2880</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>0.2880</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
<td>0.0800</td>
</tr>
</tbody>
</table>
The Numbers of the text after decoding It contain 2000 element and all of it is include error does not resemble the original numbers.
### 4.3

Average the absolute value of the difference between the elements of Matrix of The numbers after decoding and Matrix of The numbers before encryption is equal = 8.7869e-012.

The Numbers of the text after decoding and its treatment mathematically to approximated to the nearest integer it contain 2000 element and its quite similar to the original matrix and the zeros at its end which representing spaces been added at the beginning of the encryption need for programming and do not affect the content of the text.
4.4 **The text after decryption**

| This paper we will address the encryption process text is generally through a number of processes of dispersion of the later values in a matrix is A through remittances linear in addition to the use of SVD enters, including three keys sequentially, where work will begin the application process distracting initial we called (MK-Distracting the numbers method1). In a compound to generate new matrices A1 and A2 of the original text matrix and which enters the first key (Key1) and then using the second key (Key2) for a linear transform matrices A1 and A2 second phase in dispersing Numbers Matrices (MK-Distracting the numbers method2) to get the new matrices B1 and B2. The third phase of the dispersion is using SVD on the last matrices and switch S matrix among the two spectral for the new matrices C1 and C2 which represents putting as correlative $F = [C1 \, C2]$ the matrix of the initial of the encoded text. Then conducting the process of chromaticity values in the last matrix composite F, which will be values of real non-specific range that is to say including what is less than zero, including what is bigger than the one to be ultimately values of later within the closed set $[0,1]$ while retaining the largest value and the smallest value... In the matrix FF within the last matrix to ensure the possibility of return versa in the decryption phase in a way that we called (MK press numbers). The final matrix resulting matrix is the final encrypted text that we call (M.K. Text Cipher1). |

| 4.5 |
| Encryption time = 0.003 second. |
| Decryption time = 0.006 second. |

5 **CONCLUSION**

1. The encryption algorithm is a composition of 2 dispersal operations and substituted one confidential key which makes it impossible strong disassemble code the means and decoding programs currently available.
2. The level of encryption algorithm is characterized by high precision and so under standards of accuracy results used the mean of error.
3. enters the algorithm one key to entered within the matrix of text encryption phases which is a real number but not equal zero.

4. was characterized this algorithm their implementation quickly by computer compared to other encryption algorithms concerning the text.

5. alone in this algorithm is the introduction the technique of SVD within the two stages of dispersion.

6. Brought together the algorithm between three scientific fields within two specialists are: the competence of two fields in mathematics that matrix algebra and numerical analysis in addition to the competence of computers and programming language MATLAB.

6 ACKNOWLEDGEMENTS

At the conclusion of this research, I cannot but extend my thanks and gratitude to the Department of Mathematics for the moral, administrative and scientific assistance it provided me. And I also extend my thanks and appreciation to my supporter and my first assistant in my work, she is my wife, Mrs. Balqis Shrrad Hussain

REFERENCES


