EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 4/ July 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Text Encryption Based on Singular Value Decomposition

NIDHAL K. EL ABBADI
Computer Science Department
University of Kufa, Najaf
Iraq
ADIL MOHAMAD AL RAMMAHI
MOHAMMED ABDUL-HAMEED
DHEIAA SHAKIR
Mathematical Department
University of Kufa, Najaf
Iraq

Abstract:

Nowadays, text encryption is recommendable when it is transmitted or stored on insecure channels as Internet. In this paper we introduced novel method to encrypt text based on SVD. Up to our knowledge this is the first paper encrypted text by using SVD.

The message is the composition of some character. Every character of the message can be represented as an ASCII value, and then we can build numeric matrix for each text. We suggested using other text as key and using with plaintext to scramble the plaintext prior to use the SVD process which makes cryptanalyst's job difficult. There are many difficulties in using the SVD to encrypt text. The decrypted text was the same as the plaintext without loss any character. Encryption and decryption time were reasonable. One of the important features of this work is the ability to produce encrypted text with language differ from the plaintext language which make add more complixity of decrypt the encrypted text from third party.

Key words: Encryption, SVD, decryption, text.

1. Introduction

Information security is one of the most important issues to be considered when describing computer networks. The existence of many applications on the Internet, for example e-commerce (selling and buying through the Internet) is based on network security. In addition, the success of sending and receiving sensitive data using wireless networks depends on the existence of a secure communication (the Virtual Private Network, VPN). One of the methods which are used to provide secure communication is Cryptography (Ahmad Abusukhon et al. 2012).

Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc.

Public or Asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised (Ayushi, 2010).

Traditional encryption algorithms are private key encryption standards (DES and AES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC), as well as the international data encryption algorithm (IDEA).

There are other algorithms for encrypting text. Some of them use the corresponding decimal ASCII code, convert it to binary numbers and apply a process for changing the order of the bits. Another proposal is a technique on matrix scrambling which is based on random function, shifting and reversing techniques of circular queue (Elena Acevedo et al. 2013).

(Akanksha Mathur, 2012) presented an algorithm for data encryption and decryption based on ASCII values of characters in the plaintext. This algorithm is used to encrypt data by using ASCII values of the data to be encrypted. The secret used will be modifying of another string and that string is used as a key to encrypt or decrypt the data. So, it can be said that it is a kind of symmetric encryption algorithm because it uses same key for encryption and decryption but by slightly modifying it. This algorithm operates when the length of input and the length of key are same.

(Anupam Kumar Bairagi, 2011) describes how such an even-odd encryption based on ASCII value is applied and how encrypted message converting by using Gray code and embedding with picture can secured the message and thus makes cryptanalyst's job difficult.

2. Singular Value Decomposition (SVD)

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

$$A = USV^T$$

Where S is a $m \times n$ matrix with non-diagonal entries all zero and:

$$s_{11} \geq s_{22} \geq \cdots \geq s_{pp} \geq 0 \text{ where } p = \min\{m, n\}$$

Not:

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.

$$A = col_1(U)s_{11}col_1(V)^T + col_2(U)s_{22}col_2(V)^T + \cdots + col_p(U)s_{pp}col_p(V)^T \ldots (6)$$

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

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

v_j Denote column j of V.

Note: 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 $s_{jj} = \sqrt{\lambda_j}$

$\because$ V Is orthonormal matrix $\Rightarrow$ each of its columns is a unit vector.

$\therefore \|v_j\| = 1$

Thus the singular values of A are the square roots of the eigenvalues of A^TA.

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

$$\begin{bmatrix} s_{11} & 0 & \cdots & 0 & \\ 0 & s_{22} & \cdots & 0 & 0_{p,n-p} \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & s_{pp} & \\ & 0_{m-p,p} & & & 0_{m-p,n-p} \end{bmatrix}$$

$\because AV = US, so$

$$\therefore A[v_1 \quad v_2 \quad \cdots \quad v_n] = [u_1 \quad u_2 \quad \cdots \quad u_m]\begin{bmatrix} s_{11} & 0 & \cdots & 0 & \\ 0 & s_{22} & \cdots & 0 & 0_{p,n-p} \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & s_{pp} & \\ & 0_{m-p,p} & & & 0_{m-p,n-p} \end{bmatrix}$$

$$\Rightarrow Av_j = s_{jj}u_j \quad \Rightarrow \quad u_j = \frac{1}{s_{jj}}Av_j$$

3. Methodology

3.1 Encryption

In this paper we introduced new way to encrypt text based on SVD.

The first step in encryption process is to converting the plain text to the corresponding ASCII code, and then arranges these numbers as square matrix called (A).

The key is any text suggested to use as a key regardless the length of the key. The suggested key also converts to corresponding ASCII numbers and then resize and rearrange as a square matrix with the same dimension of matrix A called matrix (B).

The elements of both matrices A and B will be scrambling to create another two matrices different from the origin matrix. This can be achieved by the following steps:

1. First matrix (C1) created by multiplication the key matrix by the plaintext matrix.

$$C1 = Key.* B$$

It is clear that (Key and B) are matrices have the same dimensions and this is the multiplication between each element in the matrix (Key) with the corresponding element in the matrix B.

2. While the second matrix (C2) created by flipping the matrix C1 horizontally (so the first column of the input becomes the last column of the output).

SVD will be applied for the resulting matrices (C1 and C2)

$$[UC1, SC1, VC1] = SVD(C1) \quad ,[UC2, SC2, VC2] = SVD(C2)$$

Now, the important step introduced which reconstruct new matrices (D1 and D2) from matrices resulted from the SVD. This done by changing the (S) matrix between the matrices results from (C1 and C2), as follow:

$$D1 = UC1 * \mathbf{SC2} * VC1^T, \qquad D2 = UC2 * \mathbf{SC1} * VC2^T$$

The text matrix cipher will be (F) which is

$$F = [D1; D2]$$

Note the resulted matrix F is a real numbers matrix, these numbers will be rearranged by using specific process to represent it's with group of integer values, and then each integer number displayed as a character according to the ASCII representation, or we can suggest specific character for each number.

3.2 Decryption

The decryption algorithm is the inverse of encryption algorithm. Start with converting each character in the cipher text to the corresponding ASCII number, and then reproduce the real numbers from each group of integer numbers, the result is the matrix F.

From the matrix F we reconstruct the matrices ($D1_{new}$ *and* $D2_{new}$). SVD will be applied for both matrices ($D1_{new}$ *and* $D2_{new}$) to get:

[U$D1_{new}$, S$D1_{new}$, V$D1_{new}$]= SVD ($D1_{new}$)

[U$D2_{new}$, S$D2_{new}$, V$D2_{new}$]= SVD ($D2_{new}$)

So the C1 and C2 will be reconstructed as follow:

$$C1_{new} = \mathrm{U}D1_{new} * \boldsymbol{SD2}_{new} * \mathrm{V}D1_{new}{}^{T}$$

$$C2_{new} = \mathrm{U}D2_{new} * \boldsymbol{SD1}_{new} * \mathrm{V}D2_{new}{}^{T}$$

$$B_{new} = C1_{new}./key$$

Now the (Key and $C1_{new}$) are matrices have the same dimensions and this is the division between each element in the matrix (Key) with the corresponding element in the matrix $C1_{new}$.

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

4 The Results

We test proposed algorithm with the text in the **Fig. 1** which is written in English language.

Plaintext in English language:

Image encryption is one of the most methods of information hiding. A novel secure encryption method
for image encryption is presented in this paper. The proposed algorithm based on using singular value decomposition SVD. In this Paper we start to scramble the image data according to suggest keys (two sequence scrambling process with two different keys) to finally create two different matrices.

Figure 1: English plaintext

We test the encryption algorithm by using short key to encrypt the plaintext showed in Fig. 1. The short Key used to encryption showed in **Fig. 2**.

Short Key:

Information security is a fast growing research field which includes numerous problems

Figure 2: the key used for encryption text in Fig. 1.

Part of the encrypted text resulted from this process is showed in **Fig. 3.**

/fl|m0hdsF~JZ4I^UnAjDI{BgO;Zq|e4TBe~x/fl|m0hdsF~JZ4I^UnAjDI{BgO;Zq|e4TBe~xh9x>D<1qPR7e6;aAB6R~G]aqRcvJ79wks4MU4Lkh`Oh9x>D<1qPR7e6;aAB6R~G]aqRcvJ79wks4MU4Lkh`O]4.6 • tpi?7D^LmG9`ehk>dM3eTC]1^1v.m]hIt?Ie]4.6 • tpi?7D^LmG9`ehk>dM3eTC]1^1v.m]hIt?IeyJh]6W:i` • Z7 • <n|J~D4`enb4hYF/ • WW?YIRiR7bXyJh]6W:i` • Z7 • <n|J~D4`enb4hYF/ • WW?YIRiR7bXJytxZ6~AU;L12IhPr61vRi4{M7Ltj~ONL]7Ur7=_JytxZ6~AU;L12IhPr61vRi4{M7Ltj~ONL]7Ur7=_DDTptk~.xImypI{B_;{_X.sv;0FkiD06`3JLkLg>94RN{]7_eO]s??B[0IUOF>j_60c[>Z~NLm[R{AO3XKBX{]7_eO]s??B[0IUOF>j_60c[>Z~NLm[R{AO3XKBX;4b{iwJO{A?uTLQZ3}sBqRO|ZTekt-JPeBf----;4b{iwJO{A?uTLQZ3}sBqRO|ZTekt-JPeBf--
^vq|L7H:IK;=3;=P=JQHG<QF:PF60L139?OE=O=A3?N=6O;A9^vq|L7H:IK;=3;=P=JQHG<QF:PF60L139?OE=O=A3?N=6O;A9~K.2/6<7_PtPBDK9@PJ:8JB2M.91EPHL=B>O=7I<F9Q~-.K.2/6<7_PtPBDK9@PJ:8JB2M.91EPHL=B>O=7I<F9Q
:EDLp[X^A88MTGH9>:M3=NBK@SBLO:8P:?OF9;HQH8K>PcS:EDLp[X^A88MTGH9>:M3=NBK@SBLO:8P:?OF9;HQH8K>PcS1.K • l_ZepN9E96/K9L9:OKJ=?5N=6>;PH<RSV=KU1.K • l_ZepN9E96/K9L9:OKJ=?5N=6>;PH<RSV=KU[;]cj]3@>PA<BUOKGDn2Im`_=_z32AN@L<D6OTTTNRO;N[;]cj]3@>PA<BUOKGDn2Im`_=_z32AN@L<D6OTTTNRO;N?BEUeE89>SIK83B_WejF-

Figure 3: part of encrypted text.

The decrypted text is the same as original plaintext.

Also we test the algorithm with long key almost equal to the size of plaintext; in this case we used text written in Arabic language to prove the possibility of using this algorithm with any language, plaintext showed in **Fig. 4.**

Plaintext in Arabic Language:

كان ولا زال العراق بحاجة الى خطوات حقيقية من اجل تسريع البناء العلمي والاداري والعمراني بل وحتى البناء الانساني فمن المعروف وبحكم التجربة التي مر بها كل من عاش الجوّ الوظيفي ان الأحداث التي يمر بها الفرد خلال خدمته الوظيفية تكون مليئة بالتناقضات والمفاجآت والتي وبمحصلتها النهائية تؤدي الى عدم التعويل على موقف من المواقف او نتيجة من النتائج فكل المخرجات الادارية مرهونة بمدخلاتها ومعطياتها والأجواء المحيطة بها سلبا كانت ام ايجابا فنحن في بلد لا يزال يراوح في مجال ادارة الموارد البشرية وبحاجة الى فترة من الزمن ليست بالقليلة ليتعافى من مخلفات العقود الطويلة من التشتت في كل شيء اضافة الى حاجته الى الاستفادة من تجارب الآخرين من الشعوب التي سبقتنا في مجال التنمية الادارية وتطوير السياقات والعلاقات الوظيفية وهذا الأمر لن يحصل بين عشية وضحاها ولزاما علينا ان نتحمل المخاضات السلبية التي نتعرض اليها خلال حياتنا اليومية في مجال العمل الوظيفي او غيره من المجالات الحياتية وعلينا ان لا ننسى ان فلسفة عقيدة الانتظار تحتم علينا ان نتعامل مع تلك المخاضات السلبية بحكمة وانصاف.

Figure 4: Arabic plaintext

The key used to encrypt the plaintext showed in **Fig. 4** is also in Arabic language showed in **Fig. 5.**

Long Key:

كلية الرياضيات وعلوم الحاسوب هي واحدة من كليات جامعة الكوفة وقد تأسست في سنة 2008 بعد ان كانت قسما من اقسام كلية العلوم باسم قسم الرياضيات حيث اضيف قسم علوم الحاسوب اليها عند استحداثها وكان استحداثها ككلية مستقلة نتيجة لجهود استثنائية بذلها مؤسسها الاستاذ الدكتور المرحوم سليم الكتبي الذي كان اول عميد لها حتى تقاعده والذي خلفه الدكتور غفار حسين بصي فترة قصيرة قبل ان ينتقل الى جوار ربه بعد اصابته بمرض عضال رحمه الله .. بعد ذلك انيطت مهام ادارتها الى الدكتور يحيى الميالي حتى تقاعده نهاية سنة 2013 والآن هي تحت ادارة الاستاذ الدكتور عباس البكري الذي كان له الدور في استقرار هذه الكلية ... اشترك لفترة قصيرة في ادارة عمادتها الدكتور كاظم بريهي الجنابي ... في الكلية قسمان هما قسم الرياضيات وقسم علوم الحاسوب وفي قسم الرياضيات يوجد دراسات عليا هي دراسة الدبلوم العالي ودراسة الماجستير وفي النية استحداث دراسة الدكتوراه التي تعتبر من الدراسات العليا القليلة في البلد في مجال الرياضيات

Figure 5: encryption key.

Part of the result from this process is showed in **Fig. 6**.

xjVZ/1+=m{DxJ$/B{sh1\jy+4Ohz]+|C+;m<oFzqoG? • xjVZ /1+=m{DxJ$/B{sh1\jy+4Ohz]+|C+;m<oFzqh__M(#eSJFv5 &HS?7W • jt • A;XO7s_,tr8,oVcmOOca3zfy"XLh__M(#eS JFv5&HS?7W • jt • A;XO7s_,tr8,oVcmOOca3zfy"XLav[z VDy8Q*+G(,'M"/[`q&/==HGE6]F1;mGzQ • rjdVhW}av[z VDy8Q*+G(,'M"/[`q&_/==HGE6]F1;mGzQ • rjdVhW}$j %8 • cm@vC(9MMf$f/OOHMm%m~dZ|+]fx$j • m/X&H2 =VOm$j%8 • cm@vC(9MMf$f/OOHMm%m~dZ|+]fx$j • m/X&H2=VOm*Z=}QVCU):F]ahXMD6q/Dn"Q}o^O_+yz Tac&a~)y?4F&X • O*Z=}QVCU):F]ahXMD6q/Dn"Q}o^O _+yzTac&a~)y?4F&X • Oo1$\|:1Fv8y8&zXsf$|Zw.v • aTaF Sv&Vuy=[hA<cVqOh2o1$\|:1Fv8y8&zXsf$|Zw.v • aTaFSv &Vuy=[hA<cVqOh2")R.|4Q]f:>%|vz1OHQ.=a5:Z$4v*I&z |:$'I4V2|X"8^jo")R.|4Q]f:>%|vz1OHQ.=a5:Z$4v*I&z|:$'I 4V2|X"8^joZz*(A??Xl1)W8yZO]+J<XxHux6xqc'sJ~q_ah. JI\]HKljZz*(A??Xl1)W8yZO]+J<XxHux6xqc'sJ~q_ah.JI\] HKljqtnPd(..=K"]XaD%h|:4;$@N(HV=jF(;s&lzXsq1JGm J7JH/qtnPd(..=K"]XaD%h|:4;$@N(HV=jF(;s&lzXsq1JG mJ7JH/"Dhk/uuXq`0z • 6FiNFZxT&/%Fi5$8(8hs{HH:J • (

Figure 6: part of the encrypted text.

The decrypted text is the same as original plaintext.

Encryption and decryption times checked, also the throughput determined. The results showed in **Table 1**.

Where,

$$\text{Throughput} = \frac{\text{The size of the encrypted text in Megabyte}}{\text{The time required for encryption in seconds}}$$

5. Discussions

The encryption algorithm can use short or long text as a key efficiently, and the decrypted text retrieved the plaintext without any change in spite of using SVD algorithm which converts integer numbers to real numbers.

Also the encryption and decryption time was reasonable.

6. Conclusions

In this paper we suggest new text encryption algorithm based on using the SVD combined with other idea to scramble the text prior to encryption.

The key used in this algorithm is text with variable length or size up to the size of plain text without affecting the performance of encryption.

One of the important features of this proposed is the ability to convert the encrypted text to other language differs from the plaintext language as showed in Fig. 5, which is English text for Arabic plaintext.

Encryption and decryption time was reasonable and it is possible to reduce it when using faster computer.

Table 1: showed encryption and decryption time, and throughput.

			key										
			English						Arabic					
		Size of text K.B.	number of key characters	Size of key K.B.	Enc. time m.sec	throughput of encryption	Dec. time m.sec	throughput of decryption	number of key characters	Size of key K.B.	Enc. time m.sec	throughput of encryption	Dec. time m.sec	throughput of decryption
English	200	12.6	200	12.5	62	0.203	0.87	14.48	200	12.7	47	0.268	31	0.406
			400	12.7	46	0.274	16	0.788	400	12.8	47	0.268	31	0.406
			600	12.8	47	0.268	31	0.406	600	12.9	62	0.203	0.76	16.579
			800	12.9	46	0.274	47	0.268	800	13	78	0.162	0.23	54.783
	400	12.8	200	12.5	62	0.206	31	0.413	200	12.7	47	0.272	31	0.413
			400	12.7	47	0.272	0.98	13.06	400	12.8	47	0.272	16	0.8
			600	12.8	62	0.206	16	0.8	600	12.9	31	0.413	15	0.853
			800	12.9	47	0.272	31	0.413	800	13	47	0.272	0.86	15
	600	12.9	200	12.5	62	0.208	31	0.416	200	12.7	47	0.274	31	0.416
			400	12.7	62	0.208	16	0.806	400	12.8	47	0.274	47	0.274
			600	12.8	63	0.205	15	0.86	600	12.9	47	0.274	31	0.416
			800	12.9	62	0.208	31	0.416	800	13	47	0.274	16	0.806
	800	13	200	12.5	62	0.21	0.98	13.27	200	12.7	46	0.283	15	0.867
			400	12.7	78	0.166	31	0.419	400	12.8	47	0.276	47	0.276
			600	12.8	47	0.276	15	0.867	600	12.9	32	0.406	31	0.419
			800	12.9	47	0.276	15	0.867	800	13	47	0.276	47	0.276
Arabic	200	12.7	200	12.5	46	0.276	32	0.397	200	12.7	46	0.276	0.89	14.27
			400	12.7	46	0.276	16	0.794	400	12.8	63	0.202	47	0.27
			600	12.8	47	0.27	16	0.794	600	12.9	31	0.41	0.78	16.28
			800	12.9	46	0.276	47	0.27	800	13	47	0.27	47	0.27
	400	12.9	200	12.5	49	0.263	32	0.403	200	12.7	47	0.274	31	0.416
			400	12.7	47	0.274	0.87	14.83	400	12.8	46	0.28	47	0.274
			600	12.8	46	0.28	31	0.416	600	12.9	47	0.274	47	0.274
			800	12.9	47	0.274	0.89	14.49	800	13	47	0.274	16	0.806
	600	13	200	12.5	46	0.282	31	0.419	200	12.7	63	0.206	47	0.276
			400	12.7	47	0.276	0.69	18.84	400	12.8	47	0.276	15	0.866
			600	12.8	47	0.276	31	0.419	600	12.9	47	0.276	47	0.276
			800	12.9	78	0.166	0.78	16.66	800	13	47	0.276	31	0.419
	800	13.1	200	12.5	47	0.279	31	0.422	200	12.7	47	0.279	0.88	14.88
			400	12.7	47	0.279	16	0.819	400	12.8	46	0.285	63	0.208
			600	12.8	47	0.279	47	0.279	600	12.9	47	0.279	47	0.279
			800	12.9	63	0.208	32	0.409	800	13	62	0.211	16	0.819

REFERENCES

Abusukhon, Ahmad, Mohamad Talib, and Issa Ottoum. 2012. "Secure Network Communication Based on Text-to-Image Encryption." *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 1(4): 263-271.

Mathur, Akanksha. 2012. "An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms." *International*

Journal on Computer Science and Engineering (IJCSE) 4(9).

Bairagi, Anupam Kumar. 2011. "ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security." *IJCIT* 1(2).

Ayushi. 2010. "A Symmetric Key Cryptographic Algorithm." *International Journal of Computer Applications* 1(15).

Acevedo, Elena, Ángel Martínez, Marco Acevedo, and Fabiola Martínez. 2013. "A Novel Text Encryption Algorithm." *Research in Computing Science* 68: 91-101.