ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Use the Singular Values Decomposition in the Text Encryption with Encryption Key Is Real Number

Mohammed Abdul-Hameed Jassim Al-kufi

Teaching Assistant Lecturer, Department of Mathematical, Faculty of Computer Sciences and Mathematics,

University of Kufa, Najaf, Iraq

ABSTRACT: Cryptography is the art of achieving security by converting the message to unreadable message. This paper encrypted text based on SVD algorithm. In the first stage specific numbers suggested for each letters and punctuation characters (or using the ASCII code), and these numbers used instead of each character. The sender and receiver will agree for random real number as a key to encrypt the text. By using positive and negative key we create two new matrices which process with SVD algorithm.

Decryption is the inverse process of encryption. The encrypted text tested by using many measures and gives promised results.

KEYWORDS: Text, Encryption, SVD, Decryption.

I. 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 (Alkufi, M. 2014.).

(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

DOI: 10.15680/IJIRCCE.2016. 0402002

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.

II. SINGULAR VALUE DECOMPOSITION (SVD)

(El Abbadi, N. K. , AL-Rammahi, A.,…etc M. 2014.)(Nidhal K. El Abbadi, Adil Mohamad Al Rammahi,… etc 2015.) 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

$$A = USV^T$$

Where S is an $m \times n$ matrix with zero values for non-diagonal entries and:

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

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.

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

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.

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

$\because$ V is orthonormal matrix $\Longrightarrow$ each of it's 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, it's columns must be an orthonormal set. Hence they are linearly independent $m \times 1$ vectors.

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

$\because AV = US,$

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

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

III. METHODOLOGY

a. Encryption

The full algorithm to encrypt the text in general:

1- Suggest key which is a real number.
2- Identify the set of numbers correspond to the letters and punctuations, to replace the text with these numbers. 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.
3- By using the suggested key, two new matrix created from the original text matrix.

$$B1 = Key * A\ , \qquad\qquad B2 = -Key * A$$

4- Apply SVD algorithm for each of matrix B1 and B2.

$$[UB1, SB1, VB1] = SVD(B1)\quad , \qquad\qquad [UB2, SB2, VB2] = SVD(B2)$$

5- By changing the two singular matrix for the resulted matrix from SVD (SB1, and SB2), we create two matrix with different values.

$$C1 = UB1 * SB2 * VB1^T, \qquad C2 = UB2 * SB1 * VB2^T$$

6- Cipher text (F) build be combine the resulted two matrix.

$$F = [C1\ C2]$$

b. Decryption

1- Split the matrix ($F_{(n,\ 2m)}$) to two equal matrix $C1_{(n,\ m)}$, and $C2_{(n,\ m)}$

2- Apply SVD algorithm for each of C1, and C2 to get two matrices $B1_{new}$ *and* $B2_{new}$.

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

$B1_{new} = \text{UC}1_{new} * \text{SC}2_{new} * \text{VC}1_{new}{}^{T}$

3- $A_{new} = \frac{B1_{new}}{key}$

The last matrix A_{new} represent the numerical matrix after rounded each value.

From the last matrix we recover the letters and symbols corresponding to the numerical values suggested in encryption process.

For the purpose of the proof that each of the matrices (A) and (A_{new}) are identical we use three well-known standards of accuracy which is (MSE), (PSNR), and (Correlation coefficient).

IV. THE RESULT

4.1 The text Before encryption:-

[This paper we will address the encryption process text]

4.2 ***The numbers corresponding to the components of The text:***

84 104 105 115 32 112 97 112 101 114 32 119 101 32 119 105 108 108 32 97 100
100 114 101 115 115 32 116 104 101 32 101 110 99 114 121 112 116 105 111 110 32
112 114 111 99 101 115 115 32 116 101 120 116

Key=Any real number does not equal zero.

The code is a numerical matrix.

After decoded, the numbers are identical to the original.

4.3 The text after decryption:-

[This paper we will address the encryption process text]

Encryption time = 0.003 second.
Decryption time = 0.006 second.
MSE=0.
PSNR=∞.
Correlation coefficient=1.

V. CONCLUSIONS

a- It has very good accuracy standards using MATLAB Program as the following:

i- MSE [Between the matrix of numerical values for the original text and numerical values after decryption] = 0.

ii- PSNR [Between the matrix of numerical values for the original text and numerical values after decryption] = infinity .

iii- Correlation Coefficient [Between the matrix of numerical values for the original text and numerical values after decryption] = 1.

iv- Correlation Coefficient [Between the matrix of numerical values for the original text and numerical values for encryption matrix] = -1.

v- Mean error [Between the matrix of numerical values for the original text and numerical values after decryption] = 0

vi- NPCR = 100 % .

vii- UACI = 0 % .

b- Encryption and decryption times, and the throughput is also determined. The results shown in **table 1**. Where,

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

c- From **table(1),** the encryption and decryption time was reasonable and it is possible to be reduced with faster computers.

Table 1: Encryption and decryption time and throughput.

Plaintext	number of text characters	Size of text K.B.	Enc. Time m.sec	throughput of encryption	Dec. time m.sec	throughput of decryption
English	200	12.6	2	6.3	3	4.2
	400	12.8	3	4.266	3.5	3.657
	600	12.9	4	3.225	4.2	3.071
	800	13	3.6	3.61	3.8	3.42
Arabic	200	12.7	4	3.175	3.5	3.628
	400	12.9	3.7	3.486	4	3.225
	600	13	3	4.333	4.1	3.17
	800	13.1	4.5	2.911	3.9	3.358

d- The points of strength algorithm

i- Encryption and decryption time is very small compared to the rest encryption works.

ii- Can be applied this algorithm to encrypt any text and whatever its components and from any language.

iii- Cannot break the code by hackers because it will require a very long time up to thousands of years.

REFERENCES

1. Ahmad Abusukhon, Mohamad Talib , Issa Ottoum, Secure Network Communication Based on Text-to-Image Encryption, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 263-271.2012.
2. Akanksha Mathur, An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 09.2012.
3. Anupam Kumar Bairagi, ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security, IJCIT, VOLUME 01, ISSUE 02.2011.
4. Ayushi, A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications, Volume 1, No. 15.2010.
5. Alkufi, M. Image Encryption with Singular Values Decomposition Aided. Master Thesis for Council of Faculty of Computer Science and Mathematics. University of Kufa.2014.
6. Kolman B."Introductory Linear Algebra with Applications- Ninth Edition Bernard Kolman/ Drexel University-David R.Hill/ Temple University- Macmillan.1984.
7. El Abbadi, N. K. , AL-Rammahi, A., Alkufi, M. Image encryption based on singular value decomposition. Journal of Computer Science 10 (7): 1222-1230.2014.
8. Nidhal K. El Abbadi, Adil Mohamad Al Rammahi, Mohammed Abdul-Hameed and Dheiaa shakir, “Text Encryption Based on Singular Value Decomposition,” EDU, UoKufa, 2015.