A Novel Network Security Algorithm Based on Encrypting Text into a White-page Image

Ahmad Abusukhon, Zeyad Mohammad, and Mohammad Talib

***Abstract*—Nowadays, data security becomes a big issue and a challenge when sending sensitive data through the Internet. For example; sending user password, performing money transaction (e-business) using a master card, and invoking methods on a remote PC. All these activities require a secure algorithm for protecting data from hackers and thus keep information private and save.**

There are various methods for securing data when they are sent through the global network. Some of these techniques are based on data encryption algorithms where the text message is encrypted (scrambled) to another form that is not readable by humans. One of the encryption techniques is based on the transformation of a text into an image. In this paper, we propose a simple and a novel data encryption algorithm based on encrypting a text into a white page image (White-Page Image Encryption Algorithm or the WPI algorithm).

In this paper, the proposed White-Page Image Encryption Algorithm is tested and analyzed.

***Index Terms*— Encryption, Private Key, Secured Communication, White- Page Encryption.**

I. INTRODUCTION

Protecting sensitive data and keeping them private and secure is not an easy task when these data are sent through the Internet. This is because there are hackers in the middle between the sender and the receiver fishing data. To overcome this problem different methods for data encryption are proposed. Some of these methods focus on transforming data (e.g. text) into an image or musical notes. This paper focuses on transforming the text into an image.

Fig.1 describes how data are encrypted using a private key. As shown in Fig.1, the plain text (the text before running the encryption algorithm) is encrypted using a private key which is known to both the client and the server. Then the encrypted text is sent through a secure channel to the server. The server uses the same private key to decrypt the receiving message and gets the original message. The encryption algorithm is the algorithm used to transfer the original data (e.g. text message) into an unreadable or a hidden form [1]. The core of the encryption algorithm is a private key used by both encryption algorithm and decryption algorithm.

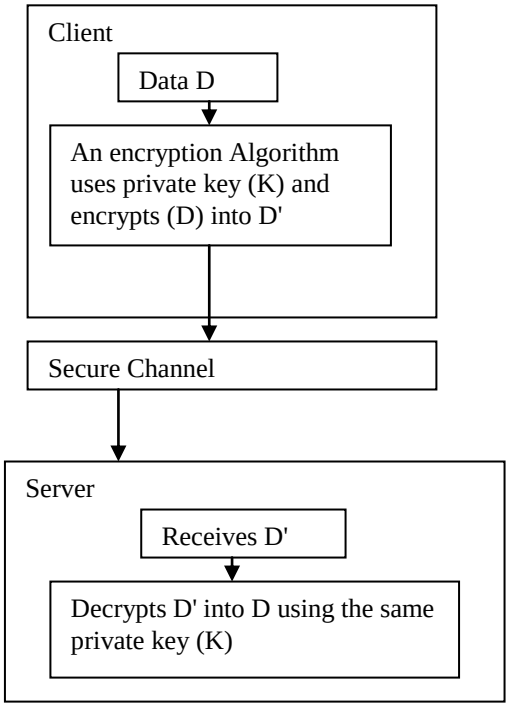

Fig. 1 The Encryption process using a private key technique

The decryption algorithm is an algorithm used for transforming the encrypted data into the original data [2], or simply, it is the encryption algorithm working in reverse.

Hackers are unauthorized users who attack the Internet in order to get sensitive data and to achieve various goals. One way to attack the Internet is to use spoofed IP address. Thus, it is essential to check the identity of the user on the Internet. There are different techniques used for verifying and validating the user's identity. These techniques include digital signature, and digital certificate [3]. Digital signature and digital certificate are not the focus of this research.

The well-known techniques used for data encryption are private key encryption (or called symmetric encryption), public-key encryption (or called asymmetric encryption), digital signature, and hash functions [4].

Manuscript received July 13, 2016; revised July 27, 2016.

Ahmad Abusukhon is with the Department of Computer Networks, Al-Zaytoonah University of Jordan, Amman, 11733 Jordan, E-mail: ahmad.abusukhon@zuj.edu.jo.

Zeyad Mohammad is with the Department of Computer Networks, Al-Zaytoonah University of Jordan, Amman, 11733 Jordan, E-mail: Z.Dosooq@zuj.edu.jo.

Mohammad Talib is with the Department of Computer Science, Khazar University, Baku, Azerbaijan, E-mail: mtalib@khazar.org

In private key encryption, both the client and the server agree on the encryption key. The encryption key is sent to the other machine using a secure channel [5].

This paper proposes a new encryption algorithm based on private-key technique.

Next, various techniques for data encryption are discussed. These techniques are focusing on image encryption, and text encryption.

Nithin, Anupkumar, and Hegde [6] proposed an image encryption algorithm (called FEAL). There technique is based on the DES encryption algorithm. In FEAL, the original image is divided into a number of blocks, then an encryption and decryption algorithms are carried out using 12 keys of size 16-bit.

M.Ali BaniYounes, and Janta[7] proposed an encryption algorithm by which an image is divided into blocks. These blocks are then reorganized into a transformed image, and then the transformed image is encrypted using the Blowfish algorithm.

Divya, Sudha, and Resmy[8] proposed to divide an image into 8 × 8 blocks. They proposed to encrypt a portion of a given image instead of encrypting the whole image to make the encryption process faster. In their algorithm, the resulting blocks are transformed from the spatial domain to frequency domain.

M.Mishra, P. Mishra, Adhikary, and Kumar [9] proposed a new method for image encryption based on Fibonacci and Lucas series.

Singh and Gilhotra [10] proposed an encryption algorithm in which a given word in a text is transformed into a floating point between 0 and 1. The resulting floating number is then transformed into a binary number that is in turn encrypted to another binary number, and then the resulting binary number is converted to a decimal number.

Huang, Chi Lee, and Hwang [11] proposed an encryption algorithm which generates n2+n common secret keys in one session.

Torkaman, Kazazi, and Rouddini [12] proposed a novel encryption algorithm which provides a secure communication while defeating the up to date attacks. There algorithm is a combination of cryptographic and steganography techniques.

Krishna [13] proposed a new mathematical model in which the output of the Elliptic Curve Cryptography (EEC) algorithm, a variable value, and a dynamic time stamp are used to generate the cipher text.

Other techniques were proposed for encrypting a text message into an image or musical notes. Some of these techniques are presented next.

Dutta,Chakraborty, and Mahanti[14] proposed an encryption algorithm which transfer the text message into musical notes using MATLAB.

Yamuna, Sankar, Ravichandran, and Harish [15] proposed to encrypt a text message into musical notes using two phases encryption algorithm. In the first phase, the text message is encrypted into a traditional Indian music and in the second phase, the Indian music notes are encrypted into western music notes.

Dutta, Kumar, and Chakraporty[16] proposed an encryption method in which each letter in the text message is transferred (mathematically) to musical notes. These musical notes and the seed value for an encryption/decryption key are sent to the receiver using the RSA algorithm.

The reset of this paper is organized as follows. Section II presents the related work. Section III presents our work, including research methodology, experiments, and the analysis of the proposed algorithm. Finally, section IV presents the conclusion and future work.

II. RELATED WORK

Bh, Chandravathi, and PRoja[17] presented Koblitz's method and used it to map a message to a point in the implementation of Elliptic Curve Cryptography [18, 19].

Singh and Gilhorta [5] proposed an encryption algorithm based on the transformation of a word of text into a floating point number (n). The resulting (n) is then encrypted into a binary number (b), and then (b) is encrypted using an encryption key.

Kumar, Azam, and Rasool[20] proposed a new technique of data encryption. In this technique, three random numbers are generated, say (r1), (r2), and (r3). The random number r1 is used for rows transformation in a matrix (M), r2 is used for columns transformation, and r3 is converted into a binary number. Rows and columns transformation is based on the value of the individual bits of that binary number.

Abusukhon and Talib [21], and Abusukhon, Talib, and Issa [22] proposed the Text-to-Image Encryption algorithm (TTIE). In their work, each letter in the text message is transferred into an individual pixel with a specific color. All pixels are then written to an image file of type "png."

Abusukhon [23] investigated using block cipher technique with the (TTIE) algorithm. In this technique, the text message is divided into a number of blocks then each block is encrypted into a sub-image. Finally, all sub-images are combined to form the final image.

Abusukhon, Talib, and Nabulsi[24] analyzed the encryption time for the TTIE encryption algorithm. The results from their work showed that the most significant time is the time required to store the encrypted data into the hard disk.

Abusukhon, Talib, and Almimi[25] proposed the Distributed Text-to-Image Encryption Algorithm (DTTIE) in order to improve the speed of the TTIE algorithm. In their work, they used a server and seven nodes working as clients. A large-scale data collection is distributed among seven nodes where each node encrypts a partition of the data collection. They evaluated the speed up of their system when a large data collection (5.77 Giga Bytes) is used.

Abusukhon and Hawashin[26] proposed a novel secure network communication protocol based on the transformation from text data to a barcode image. In their work, each letter from the alphabet list is encrypted into a

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

black bar where each bar (corresponding to a specific letter) consists of a specific number of black pixels.

Our work differs from the work presented in [21]-[25]. In their work, each letter in the plain text is encrypted and mapped into one colored pixel. In our proposed algorithm (the White-Page Image encryption algorithm, WPI) each individual letter in the text message is encrypted into an individual White pixel making it difficult for hackers to guess the encryption key. This is because hackers may think that a white page does not contain any information (no letters and no colors). In this paper we propose the WPI encryption algorithm.

III. OUR WORK

In this paper, Java NetBeans is used as a vehicle to carry out our experiments. The encryption algorithm, decryption algorithm, client program, and the server program are all implemented in java (NetBeans) and build from scratch.

A. *Machine Specifications*

All experiments in this paper are carried out using a single machine with the following specifications; processor Intel (R) core (TM)2, Duo CPU T5870 @ 2.00GHz, installed memory (RAM) 2.00GB operating system Windows 7 Ultimate and hard disk 24.5 GB (free space).

B. *Data Sample*

The data sample is created and stored in a notepad file. The data sample is shown Fig.2.

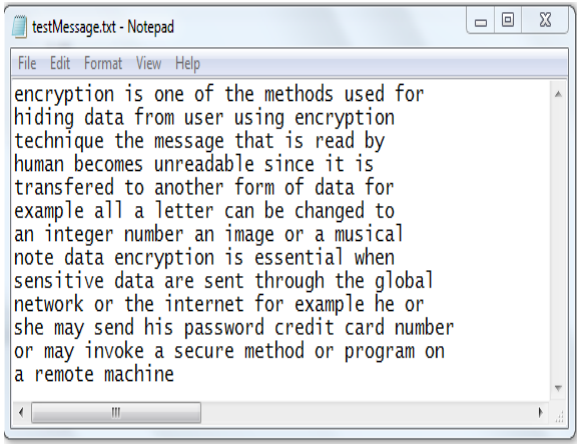

Fig. 2 Tested Data

C. *Research Methodology and Evaluation*

The plain text shown in Fig.2 is stored on the client machine. The client encrypts the plain text using the proposed algorithm (WPI) producing a White page image holding the encrypted text. The client then sends the White page image to the server machine using the loopback address (127.0.0.1) and the port number 8080. The server when receiving the cipher text decrypts it and retrieves the plain text message. The WPI encryption algorithm is evaluated by comparing the plain text on the client machine with the retrieved text message on the server.

D. *Our Experiments*

Fig.3 shows the system architecture for our experiments. The system consists of a client and a server communicating with each other using the loopback address (127.0.0.1) and a port number 8080. In other words, the client and the server are running on the same machine.

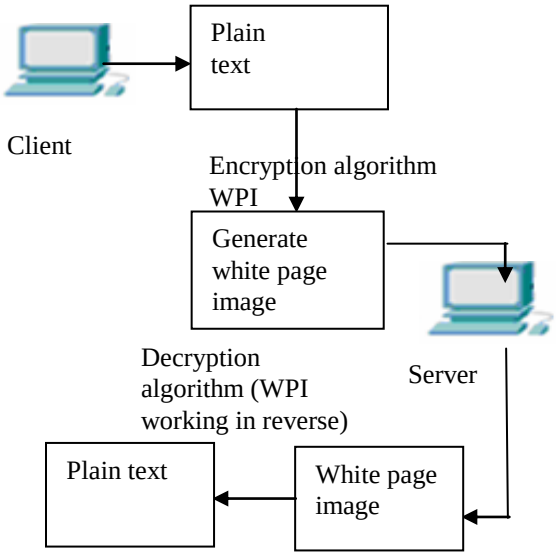

Fig. 3 The system architecture for the WPI encryption algorithm

In this experiment, the plain text shown in Fig.2 is encrypted on the client machine and sent to the server machine as a white page image (image file of type ".png") as shown in Fig.4.

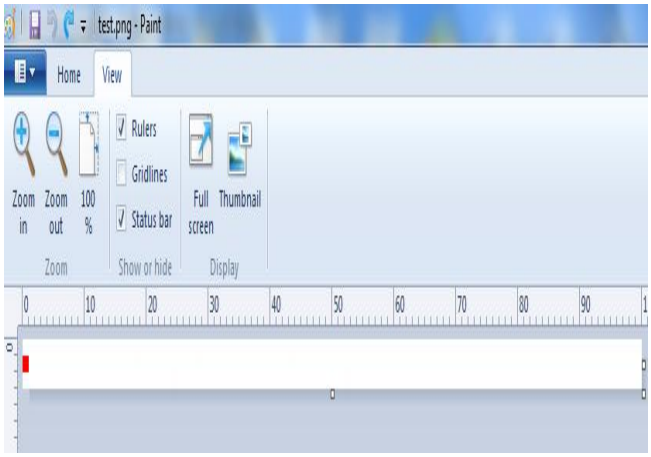

Fig. 4 The white page image results from running the WPI algorithm.

Using the proposed algorithm (WPI), each letter from the plain text is encrypted as an individual white pixel. We create a red pixel at the end of the text for clarity. The red pixel indicates the end of the encrypted text (i.e. the red pixel is neither part of the encryption algorithm nor the encrypted text).

To verify our algorithm, the client encrypts the data sample shown in Fig.2, and then the encrypted text (.png file) is sent

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

to the server. The server decrypts the ".png" file and gets the original message.

Unlike the previous work presented in [21]-[25] in this paper, each individual letter is mapped into a white pixel, of course there is a slight difference in the color density between individual white pixels, but these differences are not notable by humans. This makes it difficult for hackers to guess the key. However, in the previous work each letter is implemented by an individual color, for example, the red color represents the letter "A", the green color represents the letter "B" and so on. This could make it easier for hackers to guess the original text.

E. Analysis of the Proposed Algorithm (WPI)

In this section, the maximum number of permutations (How many times a hacker may try before he/she guesses the encryption key and gets the original text) is calculated.

The white pixel is implemented in java by three integers each has the value 255. In this experiment, we use the range from 246 to 255 to implement different densities of white pixels. For example, the letter "A" is implemented as (254,255,255), the letter "B" is implemented as (255,254,255) and the letter "C" is implemented as (255,255,254) and so on.

The range (r) = 255 -246
= 9

Thus, we have 9 different cases produce the white color. But each pixel consists of three integers and thus each case of the above 9 cases produces 3 different pixels. In other words, we have 27 cases (C) for producing the white pixels. Now, we have 26 letters (L) and each letter can be assigned to one of the 27 cases, and thus we have a number of permutations (P) where:

$$P = L \times C! \tag{1}$$

Thus, p= 26×27!

=26 × 27 × 26 × 25 × … × 1

Note that as the value of (r) is increased, the value of (P) is increased.

Note that in this paper the resulting image is a white page image. However, using WPI algorithm we can produce different color pages (i.e. red page, green page, and so on) where hackers cannot easily distinguish between different letters. This is because all letters are represented by nearly the same color (e.g. white). Fig.5 describes the WPI encryption algorithm.

// WPI encryption algorithm

Step 1: Count the letters in the plain text (say N)
Step 2: for (int c=1; c < = N; c++)
{
Step 3: Read a letter (L) from the plain text.
Step 4: Choose a white color (W) with a specific color density (in the range from 246 to 255) and stick W to L. (Note that the space between words is represented by a specific white color)
}
Step5: Create a white image of type ".png" and send it to the other end of network.

// WPI decryption algorithm

Step 1: Read the white image into a matrix (M).
Step 2: Extract the white pixels from M where each three contiguous integers represent one pixel.
Step 3: Decrypt each white pixel into a letter (Note that the space between words is represented by a specific white pixel) in order to retrieve the original message (i.e. the plain text sent by the other end of the network)

Fig. 5 The WPI encryption and decryption algorithms

IV. CONCLUSION AND FUTURE WORK

In this paper, a novel encryption algorithm, the White Page Image (WPI) encryption algorithm is proposed and tested. The WPI is based on encrypting the plain text into a white page image which is composed of white pixels slightly differs in the color density. The decryption algorithm (the WPI working in reverse) is also tested where the plain text (the original message) is produced from the white page received on the other side.

Section III-E showed that the maximum number of key permutations is limited by the value of the range available to create the white pixel in java (i.e. r).

The (WPI) algorithm could be used for off-line encryption, e-mail encryption, as well as online data encryption. In future, we propose to test the efficiency of the (WPI) algorithm when a huge data size (multi Gigabytes) is used.

ACKNOWLEDGMENT

We would like to acknowledge and extend our heartfelt gratitude to Al-Zaytoonah University of Jordan.

REFERENCES

[1] K..Lakhtaria "Protecting computer network with encryption technique: a study", *International Journal of u- and e-service, Science and Technology*, Vol. 4, No. 2, pp 43-52, 2011.

[2] A.Chan, "A Security framework for privacy-preserving data aggregation in wireless sensor networks", *ACM transactions on sensor networks*, Vol. 7, No. 4, 2011.

[3] S. Goldwasser, S.Micali, R. L.Rivest, "A Digital signature scheme secure against adaptive chosen-message attacks", *SIAM Journal of Computing*, Vol. 17, No.2, pp 281-308,1998.

[4] B. Zaidan, A.Zaidan, A. Al-Frajat, and H. Jalab, "On the differences between hiding information and cryptography techniques: an overview", *Journal of Applied Sciences*, Vol. 10, No. 15, pp 1650-1655,2010.

[5] A. Singh, R. Gilhorta, "Data security using private key encryption system based on arithmetic coding", *International Journal of Network Security and its Applications (IJNSA)*, Vol. 3, No. 3, pp. 58-67,2011.

[6] N. Nithin,M.B. Anupkumar , G. P. Hegde,"Image encryption based on FEAL algorithm", *International Journal of Advances in Computer Science and Technology*, Vol.2, No.3, pp 14-20,2013.

[7] M. Ali BaniYounes, A. Jantan, "Image encryption using block-based transformation algorithm", *International Journal of computer science (IJCS)*, Vol.35 No. 1. pp 407-415, 2008.

[8] V.V Divya, S.K. Sudha, and V.R. Resmy, "Simple and secure image encryption", *International Journal of Computer Science Issues (IJCSI)*. Vol. 9, No. 3, pp 286-289, 2012.

[9] M. Mishra, P. Mishra, M.C. Adhikary, S. Kumar, "Image encryption using Fibonacci-Lucas transformation", *International Journal on Cryptography and Information Security (IJCIS)*, Vol.2, No.3, pp 131-141, 2012.

[10] A. Singh, and R. Gilhotra, "Data security using private key encryption system based on arithmetic coding", *International Journal of Network Security and its Applications (IJNSA)*, Vol. 3, No. 3, pp 58-67,2011.

[11] L. Huang, C. Chi Lee, and M. Hwang, "A n2+n MQV key agreement protocol", *The International Arab Journal of Information Technology*, Vol. 10, No. 2, pp 137-142,2013.

[12] M.R.N. Torkaman, N.S.Kazazi, and A. Rouddini, "Innovative approach to improve Hybrid Cryptography by using DNA steganography", *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, Vol.2 No. 1, pp 224-235,2012.

[13] A.V. Krishna, "Time stamp based ECC encryption and decryption", *The International Arab Journal of Information Technology*, Vol. 11, No. 3. pp 276-281, 2014.

[14] S. Dutta, S. Chakraborty, and N.C. Mahanti, "A Novel method of hiding message using musical notes", *The International Journal of Computer Applications*, Vol. 1, No. 16. pp 76-79, 2010.

[15] M. Yamuna, A. Sankar, S.Ravichandran, and V. Harish, "Encryption of a Binary String using music notes and graph theory", *International Journal of Engineering and Technology (IJET)*, Vol. 5, No. 3. pp 2920-2925, 2013.

[16] S. Dutta, C. Kumar, and S. Chakraporty, "A Symmetric Key algorithm for cryptography using music", *International Journal of Engineering and Technology (IJET)*, Vol. 5, No. 3. pp 3109-3115,2013.

[17] P. Bh, D. Chandravathi, P.PRoja, "Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitz's method", *International Journal of Computer Science and Engineering*, Vol. 2, No. 5, pp 1904-1907, 2010.

[18] N. Koblitz, "Elliptic Curve cryptosystems", *Mathematics of computation* Vol. 48, No. 177, pp 203-209, 1987.

[19] N. Koblitz,"A Course in number theory and cryptography". 2'nd. ed. New York: Springer-Verlag,, 1994, pp 177-191

[20] K.M. Kumar, M.S.Azam, S.Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique", *International Journal of Network Security and its Applications (IJNSA)*, Vol. 2, No. 4, pp 30-41,2010.

[21] A. Abusukhon, M.Talib, "A Novel network security algorithm based on Private Key encryption", *International Conference on Cyber Security, Cyber Warfare and Digital Forensic*. Kuala Lumpur, Malaysia, Vol. 1, No. 4, pp 263-271, 2012.

[22] A. Abusukhon, M. Talib, and O. Issa, "Secure network communication based on text to image encryption", *International Journal of Cyber-Security and Digital Forensics (IJCSDF), The Society of Digital Information and Wireless Communications (SDIWC)*, Vol. 1, No. 4, pp 263-271, 2012.

[23] A. Abusukhon, "Block cipher encryption for Text-to-Image encryption algorithm", *International Journal of Computer Engineering and Technology (IJCET)*, Vol. 4, pp 50-58, 2013.

[24] A. Abusukhon, M. Talib, and M. Nabulsi, "Analyzing the efficiency of Text-to-Image encryption algorithm", *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 3, No. 11, pp 35 – 38,2012.

[25] A. Abusukhon, M. Talib, and H. Almimi, "Distributed Text-to-Image encryption algorithm", *International Journal of Computer Applications*, Vol. 106, No. 1., pp 1-5, 2014.

[26] A. Abusukhon and B. Hawashin " A Secure network communication protocol based on text to Barcode encryption algorithm", *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 12, pp 64-70, 2015.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)