International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 263-271
The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)

Secure Network Communication Based on Text-to-Image Encryption

Ahmad Abusukhon[1], Mohamad Talib[2] , Issa Ottoum[3]
[1] IT Faculty, - Computer Network Department
Al-Zaytoonah University of Jordan
Amman, JORDAN
ahmad.abusukhon@zuj.edu.jo
[2] Department of Computer Science
University of Botswana
Gaborone, BOTSWANA
talib@mopipi.ub.bw
[3]IT Faculty, - Computer Network Department
Al-Zaytoonah University of Jordan
Amman, JORDAN
Issa@zuj.edu.jo

ABSTRACT

Security becomes an important issue when secure or sensitive information is sent over a network where all computers are connected together. In such a network a computer is recognized by its IP address. Unfortunately, an IP address is attacked by hackers; this is where one host claims to have the IP address of another host and thus sends packets to a certain machine causing it to take some sort of action. In order to overcome this problem cryptography is used. In cryptographic application, the data sent are encrypted first at the source machine using an encryption key then the encrypted data are sent to the destination machine. This way the attacker will not have the encryption key which is required to get the original data and thus the hacker is unable to do anything with the session. In this paper, we propose a novel method for data encryption. Our method is based on private key encryption. We call our method Text-To-Image Encryption (TTIE).

KEYWORDS

Network; Secured Communication; Text-to-Image Encryption; Algorithm; Decryption; Private key; Encoding.

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) [11]. One of the methods which are used to provide secure communication is Cryptography.

Cryptography (or sometimes referred to as encipherment) is used to convert the plain text to encode or make unreadable form of text [9]. An Encryption method uses what is known as an encryption key to hide the contents of a plain text (make it unintelligible). Without knowing the decryption key it is difficult to determine what the plain text is. In computer networks; the sensitive data are encrypted on the sender side in order to have them hidden and protected from

unauthorized access and then sent via the network. When the data are received they are decrypted depending on an algorithm and zero or more encryption keys as described in "Fig.1".
Decryption is the process of converting data from encrypted format back to their original format [3]. Data encryption becomes an important issue when sensitive data are to be sent through a network where unauthorized users may attack the network. These attacks include IP spoofing in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP and packet sniffing in which hackers read transmitted information. One of the applications that are attacked by the hackers is the E-mail. There are many companies providing the E-mail service such as Gmail, Hotmail and Yahoo mail. These companies need to provide the user with a certain data capacity, speed access, as well as a certain level of security. Security is an important issue that we should consider when we choose Web Mail [14].

Some of the techniques that are used to verify the user identity (i.e. to verify that a user sending a message is the one who he claims to be) are the digital signature and the digital certificate [5]. Digital signature and digital certificate are not the focus of this research.

There are some standard methods which are used with cryptography such as private-key (also known as symmetric, conventional, or secret key), public-key (also known as asymmetric), digital signature, and hash functions [17]. In private-key cryptography, a single key is used for both encryption and decryption. This requires that each individual must possess a copy of the key and the key must be passed over a secure channel to the other individual [15]. Private-key algorithms are very fast and easily implemented in hardware. Therefore they are commonly used for bulk data encryption.

Mainly, there are two types of private-key encryption; stream ciphers and block ciphers [1].

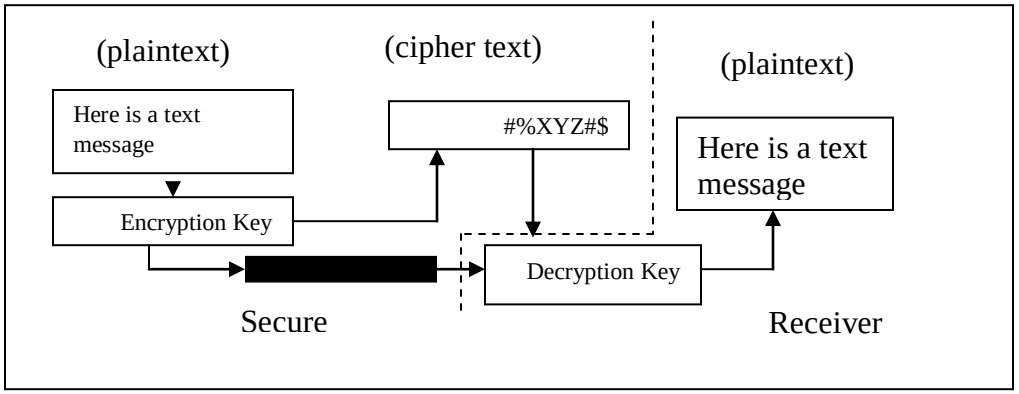

Figure 1 Encryption and Decryption methods with a secure channel for key exchange.

In stream ciphers a given text is encrypted one byte or one bit at a time whereas in block ciphers a given text is divided into chunks and then chunks are encrypted using an encryption algorithm. Example of stream ciphers are RC4 ciphers and one time pad ciphers. Examples of block ciphers are DES and AES [15].

Data encryption is performed serially or in parallel. Data encryption is performed in parallel in order to speed up cryptographic transformations. In Block ciphers algorithms such as DES there are some of the operations executed serially like CBC and CFB and other operations executed in parallel like ECB and OFB [10]. Parallel encryption is not the focus of this research. In this research we focus on stream ciphers rather than block ciphers.

The main components of the symmetric encryption include - plaintext, encryption algorithm, secret key, cipher text and decryption algorithm. The plaintext is the text before applying the encryption algorithm. It is one of the inputs to the encryption algorithm. The encryption algorithm is the algorithm used to transfer the data from plaintext to cipher text. The secret key is a value independent of the encryption algorithm and of the plaintext and it is one of the inputs of the encryption algorithm. The cipher text is the scrambled text produced as output. The decryption algorithm is the encryption algorithm run in reverse [16, 3, 14].

Public-key encryption uses two distinct but mathematically related keys – public key and private key. The public key is the non-secret key that is available to anyone you choose (it is often made available through a digital certificate). The private key is kept in a secure location used only by the user. When data are sent they are protected with a secret-key encryption that was encrypted with the public key. The encrypted secret key is then transmitted to the recipient along with the encrypted data. The recipient will then use the private key to decrypt the secret key. The secret key will then be used to decrypt the message itself. This way the data can be sent over insecure communication channels [16]. Examples on public key encryption are Pretty Good Privacy (PGP) and RSA. PGP is one of the most public key encryption methods. RSA [12] is based on the product of two very large prime numbers (greater than 10^{100}). The idea of RSA algorithm is that it is difficult to determine the prime factors of these large numbers. There are other algorithms used to create public keys such as E1Game1 and Rabin but these algorithms are not common as RSA [9].

In this paper, we propose a new data encryption algorithm based on symmetric encryption technique. We propose to encrypt a given text into an image.

2 RELATED WORK

Bh. P., et al. [2] proposed the Elliptic Curve Cryptography. In this method encoding and decoding a text in the implementation of Elliptic Curve Cryptography is a public key cryptography using Koblitz's method [7, 8]. In their work, each point on the curve represents one character in the text message. When the message is parsed each character is encoded by its ASCII code then the ASCII value is encoded to one point on the curve and so on. Our

work differs from their work. In their work they used public-key technique whereas in our work we use private key technique. They encoded each character by its ASCII value but we encode each character by one pixel (three integer values - R for Red, G for Green and B for Blue).

Singh and Gilhorta [15] proposed encrypting a word of text to a floating point number that lies in range from 0 to 1. The floating point number is then converted into binary number and after that one time key is used to encrypt this binary number. In this paper, we encode each character by one pixel (three integer values R, G and B).

Kiran et al. [6] proposed a new method for data encryption. In their method the original text (plain text) was ordered into a two-directional circular queue in a matrix say A of a given size say m x n. In their work data encryption is reliant on matrix disordering. To do so, they proposed to perform transformation operations on the rows or the columns of matrix A a number of times. They proposed three types of transformation operations to be performed on A. These operations were encoded as follows; 0 for circular left shift, 1 for circular right shift, and 2 for reverse operation. The matrix disordering was carried out by generating a positive random number say R, and then this number is converted to a binary number. The decision on which to perform rows or columns transformation was based on the value of the individual bits in the binary number. For example if the binary bit is 0 then row transformation is performed otherwise (if the binary bit is 1) column transformation is performed. To determine which transformation operation should be carried out; another random number is generated and then divided by 3. The reminder of the division is 0, 1, or 2. The reminder represents the transformation operation. In case of row transformation, two distinct rows were selected randomly by generating two distinct random numbers say R1 and R2. Another two distinct random numbers were generated c1 and c2 that represent two distinct columns. The two columns c1 and c2 were generated in order to determine the range of rows in which transformation had to be performed. After the completion of each transformation a sub-key is generated and stored in a file key. The file key is then sent to the receiver to be used as decryption key. The sub-key format is (T, Op, R1, R2, Min, Max) where:

T: the transformation applied to either row or column.

Op: the operation type coded as 0, 1, or 2, e.g., shift left array contents, shift right array contents, and reverse array contents.

R1 and R2: two random rows or columns.

Min, Max: minimum and maximum values of range for two selected R1 and R2.

3 OUR ALGORITHM

Here we describe the main features of our proposed algorithm TTIE. Our algorithm includes two main phases namely the TTIE phase (this is where our work is based) and the ISE (Image-Shuffle Encryption) phase. In the TTIE phase the plain text is transformed (encrypted) into an image. In this phase the plain text is concatenated as one string and then this string is stored into an array of characters say C. For each

character in C, one pixel of the resulting image is generated. Each pixel consists of three integers created randomly in advance and before the transformation (encryption) begins (see Fig 3-A, key 1). Each integer of the three integer values represents one color. The color value is in the range from 0 to 255. The result of this phase is a matrix, say M, in which each three contiguous columns in a given row represent one character of the original text (plain text). This is done in order to make it difficult for hackers to guess what the plain text is. To the best of our knowledge, no previous work has attempted transforming a text file into an image.

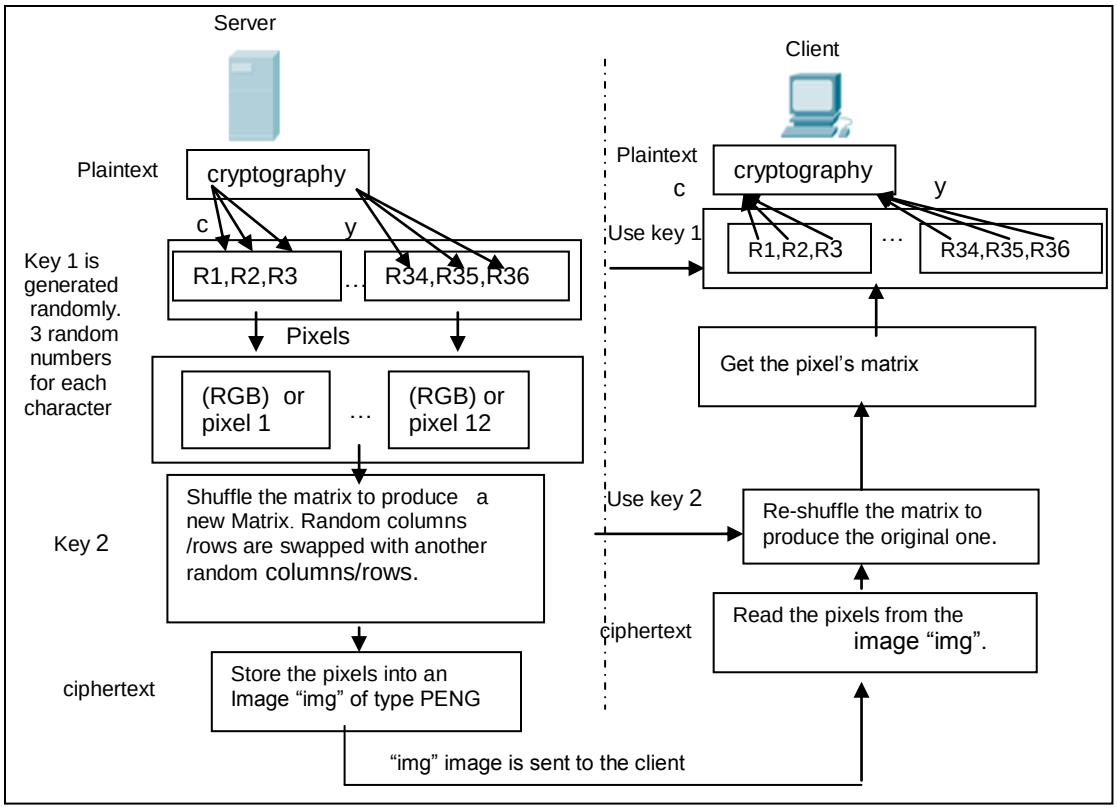

Figure 2 The main steps of the Text-to-Image-Encryption (TTIE) algorithm

The second phase is the ISE phase. The work in this phase is based on a previous work carried out by Kiran et al. [6]. In the ISE phase the matrix M is shuffled a number of times. The shuffle process includes row swapping and column swapping. In row swapping, two rows are selected randomly and then swapped. In column swapping two columns are selected randomly and then swapped. This matrix disordering makes it difficult for hackers to guess the original order of the matrix M. The shuffle key (key 2) is shown in Fig. 3-B. These two phases (the TTIE and the ISE) are carried out on the sender machine (in this paper it is the server machine) as described in Fig. 2.

The encrypted message is then sent to the client machine where the message is

decrypted using key2 and key1 respectively.

4 OUR EXPERIMENT

Java NetBeans is used as a vehicle to carry out our experiments. We build the client's and server's programs on different machines and then we tested sending and receiving data on both sides. We use the following text message in our experiments:

"encryption is the conversion of data into a form called a cipher text that cannot be easily understood by unauthorized people. decryption is the process of converting encrypted data back into its original form so it can be understood. The use of encryption decryption is as old as the art of communication in wartime. a cipher often incorrectly called a code can be employed to keep the enemy from obtaining the contents of transmissions. technically a code is a means of representing a signal without the intent of keeping it secret.

examples are morse code and ascii simple ciphers include the substitution of letters for numbers the rotation of letters in the alphabet and the scrambling of voice signals by inverting the sideband frequencies". [13].

"Fig. 3" shows part of the generated keys namely "Key 1" and "Key 2" whereas "Fig. 3" (A) shows the format of "Key 1". Each value is delimited by the # symbol. The first three values (0, 5, 5) represent one pixel in the result image. In this pixel, R (the Red color value) = 0, G (the Green color value) = 5, and B (the Blue color value) = 5. In order to guarantee that distinct letters have unique colors i.e. unique RGB values, we create 26 different ranges because of 26 alphabets. For example, these ranges are unique subsets of the main set which ranges from 0 to 255. The letter A may be represented by RGB values in the range from 0 to 9, the letter B may be represented in the range from 10 to 19 and so on. This pixel (0, 5, 5) represents the letter A. The next three values (12, 13, 17) are another pixel which represents the letter B and so on.

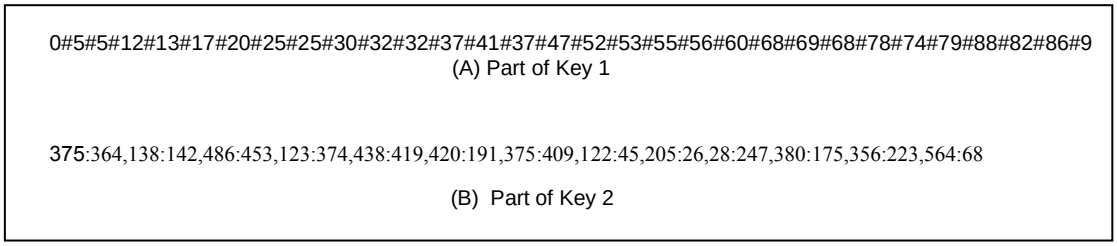

Figure 3 The format of Key1 and Key2

Figure 4 Cipher text – the output of Text-to-Image-Encryption

"Fig. 3" (B) shows the format of "Key2". Each two contiguous values represent two columns in the matrix M. The first pair in Key 2 is 375:364 which means that column number 375 is swapped with column number 364 and so on.

"Fig. 4" shows the cipher text (is the text after it is encrypted as an image). The image in Fig. 4 is zoomed out many times to make it clear. In this image pixels are created randomly and thus they do not form a known shape like tree, fish, mobile, etc. The image shown in "Fig. 4" is sent to the client and on the client side we decrypt the cipher text shown in "Fig. 4" then we finally get the original text message (i.e. the plain text).

5 ANALYSIS

In our algorithm each letter is represented by a random pixel, i.e., three random values namely R, G and B. To attack the data, hackers need to guess the following:

1. That each three contiguous values represent one letter. Since we send the data as integers' values, it is hard to guess that each three contiguous values represent one letter.
2. If a hacker is able to guess point 1, then he needs to guess what random numbers represent the letters A, B, C, etc. In other words, a hacker needs to guess the value of key 1 "Fig. 3". Note that guessing the value of key 1 is difficult since we shuffle (scramble) the matrix using key 2 (key 2 is based on the algorithm described in [6]). For example, suppose that the message we want to send is "abcd". Using key 1 "Fig. 3" (A) the random numbers generated for "a", "b", "c" and "d" are (0,5,5), (12,13,17), (20,25,25), and (30,32,32) respectively. The matrix before shuffling is described in Table-1. Table-2 describes the matrix after shuffling (Table-2 describes a simple swap operation where column 1 is swapped with column 2).

Table 1 Pixels before shuffling- each three contiguous integers in a row represent one pixel or one letter.

Letter	R-value	G-value	B-value
A	0	5	5
B	12	13	17
C	20	25	25
D	30	32	32

Table 2 Pixels after column 1 is swapped with column 2

Letter	R-value	G-value	B-value
?	5	0	5
?	13	12	17
?	25	20	25
?	32	30	32

Using statistical analysis, hackers may guess the letters from Table-1. However, it is very difficult for hackers to guess the letters from Table-2 because the order of the values RGB is changed. In other words, each three contiguous values RGB in Table-1 which represent one letter are now distributed randomly in Table-2 and thus make it difficult to guess that letter even if hackers use statistical analysis (a method involving a statistical breakdown of byte patterns such as the number of times any particular value appears in the encrypted output would quickly reveal whether any potential patterns might exist). Similarly, it is hard for "letter A follows letter B" analysis to decrypt the cipher text.

With the simple calculation, the number of possible permutations to encrypt 26 letters is-

$$((256)^3)^{26}) \quad (1)$$

Since each pixel consists of three values and each one of these values is in the

range from 0 to 255, choosing three values has $(256)^3$ permutations. We have 26 letters and thus the permutations for 26 letters is $((256)^3)^{26}$ which is equal to 1.16798479811128197597213993105 93 exp+195. The individual keys: key1 and key2, are generated each time a new message is sent. This is done in order to avoid regularity in the resultant cipher text.

6 CONCLUSION AND FUTURE WORK

In this paper, we add another level of data security at the top of the data security system proposed by Kiran et al. [6]. In our method of encryption we first encrypted the text to an image (matrix of pixels) then based on the work done by Kiran et al. [6], we scrambled the matrix to a new one making it more difficult for hackers to guess the original text message. Our algorithm is good for text encryption for a network system as well as for individual offline machines. It is also useful for e-mail security since all messages stored in the mail box will be displayed as images and thus even if someone leaves the e-mail page on it is difficult for others to guess the meaning (the original text) of these images. In future, we propose to investigate dividing the text into blocks and then transfer each block into an image and thus create an individual key for each block. This will make it difficult for hackers to use statistical approach to guess the color of each letter since different colors will be assigned to a specific letter when it appears in different blocks. In addition we will investigate the efficiency of our proposed algorithm (the TTIE) when large scale data collection (multiple Gigabytes) is used.

ACKNOWLEDGMENT

I would like to acknowledge and extend my heartfelt gratitude to Al-zaytoonah University for their financial support to carry out this work successfully.

REFERENCES

[1] Bellare, M., Kilian J., and Rogaway, P.: The Security of cipher block chaining. In Proceedings of the Conference on Advances in Cryptology (CRYPTO'94). Lecture Notes in Computer Science, vol. 839 (1994).

[2] Bh, P., Chandravathi, D., Roja, P.: Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitz's method. International Journal of Computer Science and Engineering, 2(5) (2010).

[3] Chan, A.: A Security framework for privacy-preserving data aggregation in wireless sensor networks. ACM transactions on sensor networks 7(4) (2011).

[4] Chomsiri, T.: A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test. International Journal of Computer Science and Network Security IJCSNS, 8(5) (2008).

[5] Goldwasser, S., Micali, S., L.Rivest, R.: A Digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal of Computing 17(2) pp. 281-308 (1998).

[6] Kiran Kumar, M., Mukthyar Azam, S., and Rasool, S.: Efficient digital encryption algorithm based on matrix scrambling technique. International Journal of Network Security and its Applications (IJNSA), 2(4) (2010).

[7] Koblitz, N.: Elliptic Curve cryptosystems, Mathematics of Computation, 48 (1987), pp. 203-209 (1987).

[8] Koblitz, N.: A Course in Number Theory and cryptography. 2'nd edition. Springer-Verlag (1994).

[9] Lakhtaria K. Protecting computer network with encryption technique: A Study. International Journal of u- and e-service, Science and Technology 4(2) (2011).

[10] Pieprzyk, J. and Pointcheval, D.: Parallel Authentication and Public-Key

Encryption. The Eighth Australasian Conference on Information Security and Privacy (ACISP '03). Wollongong, Australia) R. Safavi-Naini Ed. Springer-Verlag, LNCS. (2003).

[11] Ramaraj, E., and Karthikeyan, S.: A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking. Journal of Computer Science 2(9) (2006).

[12] Rivest, R.L., Shamir, A and Adelman, L.: A method of obtaining digital signatures and public key cryptosystems. Comms. ACM, 21(2) (1978).

[13] SearchSecurity , definition Encryption [online] available at: http://searchsecurity.techtarget.com/definition/encryption Accessed on 13-06-2012.

[14] Shannon, C. E.: Communication Theory of secrecy systems. Bell System Technical Journal (1948).

[15] Singh, A., Gilhorta, R.: Data security using private key encryption system based on arithmetic coding. International Journal of Network Security and its Applications (IJNSA), 3(3) (2011).

[16] Stalling, W.: Cryptography and network security principles and practices ,4th edition Prentice Hall. [online] Available at: http://www.filecrop.com/cryptography-and-network-security-4th-edition.html, Accessed on 1-Oct-2011.

[17] Zaidan, B., Zaidan A., Al-Frajat, A., Jalab, H.: On the differences between hiding Information and cryptography techniques: An Overview. Journal of Applied Sciences 10(15) (2010).