Northumbria Research Link

Northumbria
University
NEWCASTLE

A Hybrid Network Security Algorithm Based on Diffie Hellman and Text-to-Image Encryption Algorithm

Ahmad Abusukhon[1], Muhammad Naveed Anwar[2], Zeyad Mohammad[3], Bareeq Alghannam[4]
[1]Department of Computer Science, [3]Department of Computer Networks
[1,3]Faculty of Science & information Technology
Al-Zaytoonah University of Jordan,
Jordan –Amman, P.O.Box 130 Amman 11733 Jordan
[1]E-mail: ahmad.abusukhon@zuj.edu.jo, [3]E-mail:zeyad.n@zuj.edu.jo
[2]Department of Computer & Information Sciences,
Faculty of Engineering and Environment,
Northumbria University, Newcastle upon Tyne, NE2 1XE, UK.
Email: Naveed.Anwar@northumbria.ac.uk
[4]Department of Computer Science and Information System,
College of Business Studies
The public Authority for Applied Education and Training, Kuwait
E-mail:ba.alghannam@paaet.edu.kw

***Abstract* — Nowadays, the rapid growth of Internet applications open the doors for people to communicate and do business around the world and thus saving time, efforts and money. However, the success of these applications is based on protecting the data from hackers. It is well known that preventing sensitive data from hackers while they are sent through the global network is a big challenge. There are many techniques used for securing data. Some of these techniques are based on encrypting a readable text into an unreadable text using mathematical operations, while other techniques are based on encrypting a readable text into an image (e.g., the Text-to-Image Encryption algorithm – TTIE) or into musical notes using an encryption key. The encryption key must be secure and should not be sent through the Internet.**

This paper proposes adding a new security level to the TTIE algorithm, and demonstrates how the encryption key produced by the TTIE algorithm is exchanged with the other party using the Diffie Hellman technique. Thus, this paper proposes a modified TTIE algorithm called the Diffie Hellman Text-to-Image Encryption Algorithm (DHTTIE), and tests and analyses the proposed algorithm.

Subject Classification: MSC2010, 94A60

***Index Terms*— Encryption, Private Key, Secured Communication, Text-to-Image Encryption, Diffie Hellman algorithm.**

1. INTRODUCTION

The great revolution in digital data communications leads to many researches on how to achieve a high level of reliability and secrecy when transmitting the data through the Internet. One way to keep data secure is by using cryptography. Cryptography is a technique used to protect the sensitive data from hackers while they are sent through the global network by encrypting the text message from readable form into unreadable form [1]. Some of the encryption techniques focus on encrypting data into musical notes or into an image. This paper proposes a hybrid encryption technique based on the Text-to- Image encryption algorithm (TTIE) and the Diffie Hellman technique. It describes how can they work together in order to produce a more secure encryption algorithm. Fig.1 describes how data are encrypted using a private key. The private key encryption algorithms rely on the fact that both the client and the server know and own the same encryption key. As described in Fig.1, on the client side, the plain text (the message D) is encrypted using a private key into an unreadable form D' before sending it through the secure channel. The server uses the same private key to decrypt the receiving message and gets the original message.

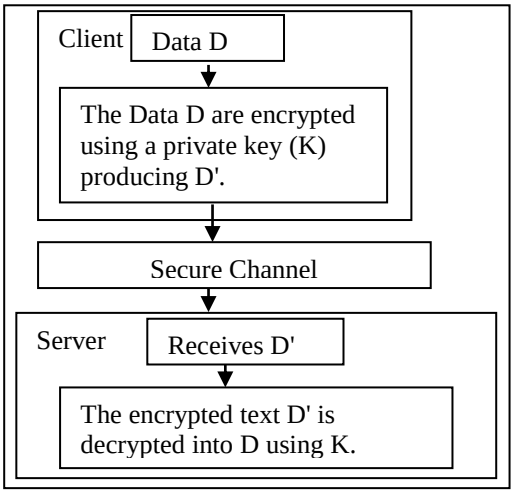

Fig. 1 The Encryption process using a private key technique

The encryption algorithm is an algorithm used to encrypt the data D into D'. In other words, the encryption algorithm is the algorithm used to transfer the original data D into an unreadable or a hidden form D' [1]. The private key (K) is

the core of the encryption algorithm. The decryption algorithm is the encryption algorithm running in reverse. In other words, the decryption algorithm is an algorithm used for transforming the encrypted data (the ciphertext) into the plaintext [2].

Encryption techniques are used to prevent hackers from accessing sensitive data when they are sent through the Internet. Examples of these techniques include digital signature, and digital certificate [3]. Digital signature and digital certificate are not the focus of this research.

Mainly, there are two techniques used for data encryption: namely private key and public-key encryption [4]. Other techniques include digital signature, and hash functions [5]. This paper focuses on private key encryption. It proposes a hybrid encryption algorithm based on the TTIE encryption algorithm and Diffie Hellman technique called Diffie Hellman Text-to-Image Encryption Algorithm (DHTTIE). Details of these techniques are given in section 3.

Below, we describe various techniques for data encryption. These techniques focus on text encryption and image encryption algorithms.

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

M.Ali, BaniYounes, and Janta [7] proposed dividing an image into a number of blocks. These blocks are then re-organized 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. In this technique, portions of an image are encrypted instead of encrypting the whole image at once. This is done in order to make the encryption process faster.

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 that encrypts a text in four phases. In this algorithm a given word in a text is transformed into a floating point between 0 and 1.

Huang, Chi Lee, and Hwang [11] proposed an encryption algorithm in which n^2+n common secret keys are generated in one session.

Torkaman, Kazazi, and Rouddini [12] proposed a novel encryption algorithm which is a hybrid 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 encrypt the data as musical notes or an image. Some of these techniques are described below.

Dutta, Chakraborty and Mahanti [14] proposed to encrypt a given plain text into musical notes using MATLAB.

Yamuna, Sankar, Ravichandran, and Harish [15] proposed two phases encryption algorithm for transforming a plain text into musical notes.

Dutta, Kumar, and Chakraporty [16] proposed an encryption algorithm in which the letters in a text message are encrypted (mathematically) to musical notes.

The rest of this paper is organized as follows. Section II, presents the previous work related to the proposed algorithm. 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.

2. 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 in a 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, a matrix (N) is encrypted by three operations namely row transformation, column transformation, and decimal to binary transformation.

Abusukhon and Talib [21], and Abusukhon, Talib, and Issa [22] proposed the Text-to-Image Encryption algorithm (TTIE). In their work, a plain text is encrypted into an image of type “png” using java.

Abusukhon [23] investigated using block cipher technique with the TTIE algorithm.

Lokeshwari et al.[24] proposed to encrypt an image by converting the image into a stream of pixels which are decomposed into blocks and then the resulted pixels are rotated based on angles. A replace code is generated for each block and then this code is encrypted using Merkle-Helman crypto system.

Abusukhon, Talib, and Nabulsi [25] analyzed the encryption time for the TTIE encryption algorithm. Abusukhon, Talib, and Almimi [26] proposed the Distributed Text-to-Image Encryption Algorithm (DTTIE) in order to improve the speed of the TTIE algorithm. Abusukhon and Hawashin [27] proposed a novel secure network communication protocol based on encrypting a plain text into a barcode image.

This work differs from the work presented in [21]-[23], [25]-[27]. In their work, each individual letter from the alphabet set is encrypted into an individual pixel (each pixel consists of three integers R, G, B). The resulting pixels (26 pixels since there are 26 English letters) represent the encryption key. The encryption key itself is sent through a secure channel to the other side. In our proposed algorithm, there is no need to send the encryption key itself to the other side. Instead, random numbers are sent to the receiver from

which a private key (k1) is generated based on the TTIE and Diffie Hellman. The result of this process is two identical keys k1 (generated on the receiver) and k1′ (generated on the sender). To achieve this goal, we use the Diffie Hellman key exchange algorithm [28]. In addition, in this paper we propose an enhanced TTIE algorithm. In this algorithm, an additional level of encryption based on RGB values is added to the existing TTIE algorithm.

Singh and Jain [29] proposed an enhanced Image to Text Encryption algorithm proposed in [21]. In their algorithm the plaintext is encrypted using the Text to Image encryption algorithm and then the resulting image is encrypted using the Advanced Encryption Standard (AES) technique. Two keys (key1 and key2) are generated and included in the encrypted image. A random number is included as a pixel in the end of the encrypted image and then this number is used to lookup the keys (key1 and key2) from a database on the receiver.

Manjunath, S.G.Hiremath [30] proposed an encryption algorithm consisting of two levels of encryption. In the first level the RSA algorithm is used to hide data and then merge them to cover image using the H-LSB technique. In the second level of encryption, Chaos algorithm encrypts the resulting image.

Arun, Azarudeen and Nivek [31] proposed an encryption algorithm based on the TTIE algorithm proposed in [21] and the AES algorithm. In their algorithm, three input values are entered and the plaintext is transformed into its ASCII code. The ASCII code values are multiplied by the user inputs and the product values are divided by 256. If the quotient value is less than 256 then it is stored otherwise, the quotient value is again divided by 256. This process produces an image and then this image is encrypted by AES algorithm using a key to produce another image.

3. THE PROPOSED WORK

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

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).

3.1 Data Sample

A small data sample is used in order to test the proposed encryption algorithm as described in Fig2. The data sample is stored in a notepad file.

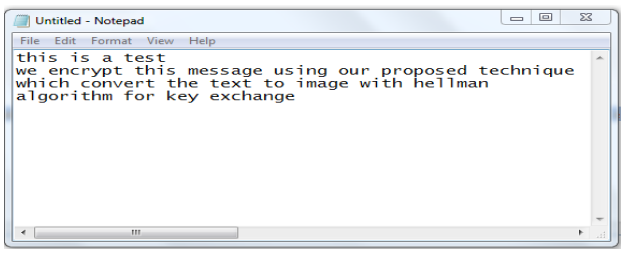

Fig. 2 The Data Sample

3.2 Research Methodology and Evaluation

In this section we use the following abbreviations:

P_L: is the plaintext.

P: is a pixel consists of three integers R, G, and B. The three integers represent the intensity of the Red, Green, and Blue colors of the pixel P.

CIP: is the ciphertext plane (a plane that represents a part of the total ciphertext) and it consists of a number of pixels.

COP: the correction plane (is the other part of the total ciphertext). Note that the CIP size and the COP size are identical. In other words, they contain the same number of pixels. However, unlike CIP, the COP plane consists of one color only while the CIP consists of multiple colors.

FEP: is the final encryption plane and is produced by performing an arithmetic operation (e.g. summation , xor, .., etc) on both planes CIP and COP.

CKP: is the key of the correction plane (this key is used for producing the correction plane COP).

CIKP: is the key of the ciphertext plane (this key is used for producing the ciphertext plane CIP).

L: is a letter from the alphabet set.

n1, n2 and n3: are random numbers.

m: the number of letters in the alphabet set.

DH: is the Diffie Hellman Algorithm.

S: is the sender node.

C: is the receiver node.

The first phase of our proposed algorithm is to perform the key exchange between the client and the server using The Diffie Hellman key exchange algorithm. In this phase random numbers are generated to produce the keys K1 and K2. The values of the generated random numbers are limited to the range from 0 to 200. This means that all values in the CIP are ranged from 0 to 200. This step produces two identical encryption/decryption keys (K1 and K2) on both sides of the network. In other words, a symmetric key encryption technique is used here. Using K1 and K2, we are able to produce the ciphertext (CIP) on both sides of the network.

In the second phase of our proposed algorithm, the Diffie Hellman key exchange algorithm is used again to produce three random numbers (R, G and B) on both sides of the network. The three random numbers represent the color of the COP. The values of the generated random numbers of the COP are limited to the range from 0 to 55.

In the third phase of our proposed algorithm (the Diffie Hellman Text to Image Encryption algorithm (DHTTIE)), the TTIE is enhanced by adding another level of encryption (the COP) to the CIP level. In other words, the resulting plane RP=CIP + COP. This is done in order to make it harder for hackers to get the plaintext. Note that the values of the COP and the values of CIP are both generated using the Diffie Hellman key exchange algorithm and they are not sent through the network.

The following is a mathematical description for the proposed algorithm DHTTIE. Here, we describe the main phases of the DHTTIE.

Phase 1: Key Exchange for the ciphertext plane (CIP)

For each L in the plaintext, S generates three secret integers namely n1, n2 and n3 and then uses the DH technique to produce one pixel consists of R, G and B values as follows:

S: Generate three random numbers (n1), (a) and (h).

S: Compute A= $(n1)^a$ (mod h)

S: Send the A value to C.

C: Generate random number (b)

C: Compute B= $(n1)^b$ (mod h)

C: Send the B value to S.

S: Compute A' = B^a (mod h)

C: Compute B' = A^b (mod h)

The result of this step is two identical numbers A' and B'. These two numbers represent the red color (R) on both S and C. In other words, R =A' = B'. Bear in mind that the R value is in the range from 0 to 200.

The above algorithm is repeated for the other two colors G and B producing for example, A″ , B″, A‴ , B‴, such that: G= A″ = B″ and B = A‴ , B‴ . Note that the three values R, G and B produce one pixel (Ω) which represents one letter from the alphabet list. Note that the values R, G and B are generated using the DH algorithm and thus they are not reveal to anyone.

To be sure that all pixels are in the range from 0 to 200, the modulus operation is used as follows:

$$R = R \% 200 , \quad G = G \% 200, \quad B = B \% 200$$

The above steps are repeated for all letters in the alphabet set producing the CIKP key. The CIKP key entries adhere to the following rule:

$$\forall L_i \; \exists ! \; P_i \; (R_i, G_i, B_i)$$

Now, suppose that (Ω) is a pixel in the CIP plane where (Ω) = {RΩ, GΩ, BΩ} and that (υ) is a pixel in the COP plane where (υ) = {Rυ, Gυ, Bυ}. In this paper we enhance the TTIE algorithm by adding (Ω) to (υ) and thus produce a new pixel (∂). Note that the values R, G and B of (∂) are in the range from 0 to 255. This is because (Ω) values are in the range from 0 to 200 and (υ) values are in the range from 0 to 55. Now, (∂) represents one pixel in the FEP plane where ∂ = {R∂, G∂, B∂}. The (Ω) values are added to the (υ) values before sending them through the channel as follows:

$$FEP = \{\partial_1, \partial_2, \partial_3, \ldots, \partial_{\text{No of pixels in the plain}}\}$$

$$FEP = \{[(R_{\Omega 1} + R_{\upsilon 1}), (R_{\Omega 2} + R_{\upsilon 2}) + (R_{\Omega 3} + R_{\upsilon 3})],$$
$$[(R_{\Omega 4} + R_{\upsilon 4}), (R_{\Omega 5} + R_{\upsilon 5}) + (R_{\Omega 6} + R_{\upsilon 6})],$$
$$[(R_{\Omega 7} + R_{\upsilon 7}), (R_{\Omega 8} + R_{\upsilon 8}) + (R_{\Omega 9} + R_{\upsilon 9})], \ldots\} \quad (1)$$

Where,

$$\partial_1 = [(R_{\Omega 1} + R_{\upsilon 1}), (R_{\Omega 2} + R_{\upsilon 2}) + (R_{\Omega 3} + R_{\upsilon 3})]$$

$$\partial_2 = [(R_{\Omega 4} + R_{\upsilon 4}), (R_{\Omega 5} + R_{\upsilon 5}) + (R_{\Omega 6} + R_{\upsilon 6})],$$

and so on.

This is done in order to make it difficult for hackers to get the plaintext. Note that the addition operation in Eq. 1 can be replaced with any arithmetic operation. Bear in mind that on the other side of the network when the receiver receives the FEP plane, it first subtracts the COP from the CIP as follows:

$$FEP' = \{[(\partial_1 - R_{\upsilon 1}), (\partial_1 - R_{\upsilon 2}) + (\partial_1 - R_{\upsilon 3})],$$
$$[(\partial_2 - R_{\upsilon 4}), (\partial_2 - R_{\upsilon 5}) + (\partial_2 - R_{\upsilon 6})],$$
$$[(\partial_3 - R_{\upsilon 7}), (\partial_3 - R_{\upsilon 8}) + (\partial_3 - R_{\upsilon 9})], \ldots\} \quad (2)$$

Then, the final phase of this algorithm is carried out where the decryption algorithm is executed in order to get the plaintext. In this phase, each three contiguous integers are grouped in order to produce an individual letter from the plaintext. Fig. 3 describes the above phases.

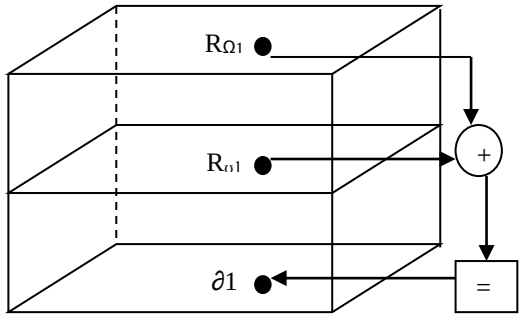

Fig. 3 The Phases of the DHTTIE encryption algorithm

The proposed algorithm (DHTTIE) is evaluated by comparing the decrypted text on the client side with the plaintext sent by the server.

3.3 Our Experiment

Fig.4, shows the system architecture for our experiment. Java (Netbeans) is used as a vehicle to carry out the experiment. The client program, the server program, the encryption algorithm and the decryption algorithm are built from scratch. The client and the server are tested on the same machine using the loopback address 127.0.0.1 and port 7070.

Fig. 4 The system architecture for the DHTTIE encryption algorithm

In this experiment, the plaintext shown in Fig.2 is encrypted on the client machine and then sent to the server machine as an image of type ".png" as shown in Fig.5.

Fig. 5 The ciphertext produced by DHTTIE algorithm

Unlike the previous work presented in [21]-[27] in this paper, the TTIE algorithm is enhanced by another level of encryption (the COP plane). In addition, the encryption keys (set of pixels) are generated on the sender and the receiver nodes and thus, there is no need to send them through the network.

3.4 Analysis of the Proposed Algorithm (DHTTIE)

The hackers need to pass through two levels of obstacles. The first level is the transformation of the text into "png" image (need to pass through the CIP and the COP planes). The second level is the Diffie Hellman level. Three integers are generated in order to produce the COP color; where each integer has a value in the range from 0 to 55. Each integer can be represented by 55 different values thus, the number of permutations checked out in order to guess the key for the COP is:

$$Pcop = (55)^3 \quad (3)$$

The number of permutations checked out before the hackers guess the CIP is:

$$Pcip = ((255)^3)^{26} \quad [22] \quad (4)$$

The key space for Pcop and Pcip (called Ksp) is the all possible permutations of an encryption key. Thus, Ksp is calculated as follows:

$$Ksp = (55)^3 \times ((255)^3)^{26} = 8.535366 \text{ e} + 192 \quad (5)$$

To calculate the number of permutations for Diffie Hellman when using the TTIE algorithm, first the key size of the proposed algorithm is calculated as follows:

We assume that the plaintext consists of the alphabet letters only (no digits or special characters are used) and thus, the number of letters (L) used for generating the plaintext is 26 letters. Since each letter is represented by three integers (I=3) and each integer is represented by eight bits (b=8), then the following equation describes the key size (S):

$$S = L \times I \times b = 26 \times 3 \times 8 = 624\text{bits} \quad (6)$$

To find the equivalent case-base for Diffie Hellman (for symmetric key encryption) we use the following equation:

$$0.05 * (SL + 14)^3 / (\log2 (SL + 14))^2 \quad (7)$$

Where, SL is the security level for symmetric encryption. [32].

Since we have a 624 bit key's size, then substituting SL = 65 in the above equation will produce a key of size = 620 bits which is very close to 624 bits key size. Thus the total number of permutations for Diffie Hellman using the proposed key (called Ksdh), is approximately:

$$Ksdh = 2^{(65)} = 36893488147419103232 \quad (8)$$

Eq. 9, describes the total number of permutations (Tp).

$$Tp = Ksp * Ksdh \quad (9)$$

Thus Tp is approximately =
3.1489941982705027534465953480025 e +212

CONCLUSION AND FUTURE WORK

In this paper, a hybrid encryption algorithm (called the DHTTIE) is proposed. The DHTTIE is based on the TTIE encryption algorithm and the Diffie Hellman algorithm. The DHTTIE is analyzed and the results showed that the total number of permutations is approximately:

3.1489941982705027534465953480025 e +212

Enhancements are carried out on the TTIE encryption algorithm by adding a new level of security (COP). This paper showed how the Diffie Hellman algorithm is used as a vehicle for generating the TTIE's key entries (colored pixels) on both sides of the network without a need for sending the key through the network. This is done in order to keep the keys secret. The proposed technique is evaluated by decrypting the message sent by the sender and thus retrieving the original message. In future, we proposed to investigate the DHTTIE when the key size is greater than 624bits and the tested data is a large-scale collection (multiple GBytes).

ACKNOWLEDGMENT

This work was supported by Al-Zaytoonah University of Jordan. We would like to acknowledge and extend our gratitude to them for their financial aid.

REFERENCES

[1] Lakhtaria,K. (2001) Protecting computer network with encryption technique: a study. *International Journal of u- and e-service, Science and Technology*. ,4, 43-52.
https://link.springer.com/chapter/10.1007/978-3-642-20998-7_47

[2] Chan, A.A Security framework for privacy-preserving data aggregation in wireless sensor networks. *ACM transactions on sensor networks*. ,7. http://dl.acm.org/citation.cfm?id=1921623

[3] Goldwasser, S., Micali, S., Rivest, R. L. (1998) A Digital signature scheme secure against adaptive chosen-message attacks, *SIAM Journal of Computing*., 17, 281-308.
http://epubs.siam.org/doi/abs/10.1137/0217017?journalCode=smjcat

[4] Zaidan, B., Zaidan, A., Al-Frajat, A. and Jalab, H. (2010) On the differences between hiding information and cryptography techniques: an overview. *Journal of Applied Sciences*., 10, 1650-1655.
http://www.oalib.com/paper/2734429.

[5] Singh, A., Gilhorta, R. (2011) Data security using private key encryption system based on arithmetic coding. *International Journal of Network Security and its Applications* (IJNSA)., 3, 58-67.
https://pdfs.semanticscholar.org/96c0/be3d7374c426723cc62d43b63ac6624db413.pdf.

[6] Nithin, N., Anupkumar , M.B. and Hegde G. P. (2013) Image encryption based on FEAL algorithm. *International Journal of Advances in Computer Science and Technology*., 2, 14-20.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.302.8504

[7] BaniYounes, M. Ali and Jantan, A. (2008) Image encryption using block-based transformation algorithm. *International Journal of computer science (IJCS)*., .35, 407-415.

http://www.iaeng.org/IJCS/issues_v35/issue_1/IJCS_35_1_03.pdf

[8] Divya, V.V, Sudha, S.K. and Resmy, V.R. (2012) Simple and secure image encryption. *International Journal of Computer Science Issues* (IJCSI)., 9, 286-289.

https://www.academia.edu/7885840/Simple_and_Secure_Image_Encryption

[9] Mishra, M., Mishra, P., Adhikary, M.C. and Kumar,S. (2012) Image encryption using Fibonacci-Lucas transformation. *International Journal on Cryptography and Information Security (IJCIS)*., 2, 131-141.

https://arxiv.org/abs/1210.5912

[10] Singh, A. and Gilhotra, R. (2011) Data security using private key encryption system based on arithmetic coding. *International Journal of Network Security and its Applications (IJNSA)*., 3, 58-67.

https://pdfs.semanticscholar.org/96c0/be3d7374c426723cc62d43b63ac6624db413.pdf.

[11] Huang, L. Chi Lee, C. and Hwang, M. (2013) A n^2+n MQV key agreement protocol. *The International Arab Journal of Information Technology*., 10, 137-142.

http://ccis2k.org/iajit/PDF/vol.10,no.2/2-3015.pdf

[12] Torkaman, M.R.N. Kazazi, N.S. and Rouddini, A. (2012) Innovative approach to improve Hybrid Cryptography by using DNA steganography. *International Journal on New Computer Architectures and Their Applications (IJNCAA)*., 2, 224-235.

https://pdfs.semanticscholar.org/d738/2a91716926cd978f2ca341cbad7964504177.pdf.

[13] Krishna, A.V. (2014) Time stamp based ECC encryption and decryption. *The International Arab Journal of Information Technology*., 11, 276-281.

http://ccis2k.org/iajit/PDF/vol.11,no.3/4571.pdf

[14] Dutta, S., Chakraborty, S. and. Mahanti, N.C. (2010) A Novel method of hiding message using musical notes. *The International Journal of Computer Applications*., 1, 76-79.

http://www.ijcaonline.org/archives/number16/338-510

[15] Yamuna, M. , Sankar, A. Ravichandran, S. and Harish, V. (2013) Encryption of a Binary String using music notes and graph theory. *International Journal of Engineering and Technology (IJET)*., 5, 2920-2925.

http://connection.ebscohost.com/c/articles/93330833/encryption-binary-string-using-music-notes-graph-theory.

[16] Dutta, S. Kumar, C. and Chakraporty, S. (2013) A Symmetric Key algorithm for cryptography using music. *International Journal of Engineering and Technology (IJET)*., 5, 3109- 3115.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.411.4160

[17] Bh, P., Chandravathi, D., PRoja, P. (2010) 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, 1904-1907.

https://pdfs.semanticscholar.org/bc2f/1260888bfb5e83a8f14bfc296a9f3fa8c87f.pdf.

[18] Koblitz, N. (1987) Elliptic Curve cryptosystems. *Mathematics of computation*., 48, 203-209.

http://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/

[19] Koblitz, N. (1994) *A Course in number theory and cryptography*. Springer-Verlag,, New York.

http://plouffe.fr/simon/math/A%20Course%20in%20Number%20Theory%20and%20Cryptography.pdf

[20] Kumar, K.M., Azam, M.S. Rasool, S. (2010) Efficient digital encryption algorithm based on matrix scrambling technique. *International Journal of Network Security and its Applications (IJNSA)*., 2, 30-41.

http://airccse.org/journal/nsa/1010ijnsa03.pdf.

[21] Abusukhon, A., Talib, M. (2012) A Novel network security algorithm based on Private Key encryption. *Proceeding of International Conference on Cyber Security, Cyber Warfare and Digital Forensic*, 26-28 June, pp. 263-271, IEEE Xplore.

http://www.iaeng.org/publication/WCECS2016/WCECS2016_pp410-414.pdf.

[22] Abusukhon, A. Talib, M. and Issa, O. (2012) 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)*. ,1, 263-271.

https://www.scribd.com/document/208597964/Secure-Network-Communication-Based-on-Text-to-Image-Encryption.

[23] Abusukhon, A. (2013) Block cipher encryption for Text-to-Image encryption algorithm. *International Journal of Computer Engineering and Technology (IJCET)*., 4, 50-58. https://www.academia.edu/3807391/BLOCK_CIPHER_ENCRYPTION_FOR_TEXT_TO_IMAGE_ALGORITHM.

[24] Lokeshwari, G. , Susarla, S. & Kumar, S. Udaya "A Modified Technique for Reliable Image Encryption Method using Merkle-Hellman Cryptosystem and Rsa Algorithm". Journal of Discrete Mathematical Sciences and Cryptography, Vol 18,No3, ,2015.

[25] Abusukhon, A., Talib, M., and Nabulsi, M. (2012) Analyzing the efficiency of Text-to-Image encryption algorithm. *International Journal of Advanced Computer Science and Applications (IJACSA)*. , 3, 35 – 38.

https://www.researchgate.net/profile/Ahmad_Abusukhon/publication/282656545_Analyzing_the_Efficiency_of_Text-to-Image_Encryption_Algorithm/links/561659d308ae2467f6863420.pdf.

[26] Abusukhon, A., Talib, M. and Almimi, H. (2014) Distributed Text-to-Image encryption algorithm. *International Journal of Computer Applications*., 106, 1-5.

http://research.ijcaonline.org/volume106/number1/pxc3899518.pdf.

[27] Abusukhon A.and Hawashin B. (2015) A Secure network communication protocol based on text to Barcode encryption algorithm. *International Journal of Advanced Computer Science and Applications*. ,6, 64-70.

http://thesai.org/Downloads/Volume6No12/Paper_9-A_Secure_Network_Communication_Protocol_Based_on_Text.pdf.

[28] Diffie W. and Hellman M. E. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*. IT-22, 644-654.

http://liris.cnrs.fr/~rthion/files/Enseignement/M2Com/ExemplesArticles/Diffie76.pdf.

[29] Singh, S. and Jain, A. ( ) Combination of RGB substitution for text to image encryption technique using AES. Spvryan's *International Journal of Engineering Science & Technology (SEST)*. ,2.

http://spvryan.org/archive/issue2volume2/01.pdf.

[30] Manjunath, N. and Hiremath, S.G. (2015) Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique". *International Journal of Electrical, Electronics and Computer Systems (IJEECS).* Vol. 3, No. 5 pp 5-9, 2015.

http://www.techrepublic.com/resource-library/whitepapers/image-and-text-steganography-based-on-rsa-and-chaos-cryptography-algorithm-with-hash-lsb-technique/.

[31] Arun , M., Azarudeen S. Mohamed and Nivek, T.N. "AES based Text to Pixel Encryption using Color Code Conversion by Modulo Arithmetic". *International Journal of Recent Research in Science, Engineering and Technology*. Vol. 1, No. 3 pp 37-42, 2015.

https://www.ijrrset.com/upload/2015/june/2-AES-Modified.pdf.

[32] https://crypto.stackexchange.com/questions/32668/diffie-hellman-key-size-to-symmetric-formula/32671. [Accessed on 1-06-2017].