International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 2, Issue 5, Nov 2013, 73-80

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

TEXT – TO – IMAGE ENCRYPTED TRANSFORMATION (TIET)

MOHAMMED ABDULRIDHAHUSSAIN

Department of Computer Science, College of Education for Pure Science, Basrah University, Basrah, Iraq

ABSTRACT

Information security means protecting information from attackers. Thus cryptography is the way to protect that information through encrypting. The complexity of the encryption process will make the attacker job more sophisticated and complex. However complexity does not means complex mathematical expression, which consumes the processor time. Meanwhile, combination of cryptography technique will result some sort of complexity.

The propose algorithm will combine a simple substitution method and transposition method. The substitution method is used to change the original pixel value. Thus transposition method will be used to detect the location of the resultant value in the image. The algorithm will named as Text – to – Image Encrypted Transformation (TIET)

KEYWORDS: Cryptography, Encryption, Network Security, Text-to-Image, Transposition

INTRODUCTION

With the rapid growth of Internet, global information tide expends the application of information network technology. It also brings about great economic and social benefit along with the extensive use of this technology. However, because Internet is an open system which faces to public, it must confront many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet [3]. Cryptography is one of the ways to protect the information in the Internet and to provide safety communication between the users.

Cryptography is a word with Greek origins, means "secret writing". However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Although in the past cryptography referred only to the encryption and decryption of messages using secret keys [2]. Now a day Cryptographic systems are characterized along three independent dimensions:

- The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged.
- The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
- The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along [1].

Security Goals: When we talk about computer security, we mean that we are addressing three important aspects of any computer-related system: Confidentiality ensures that computer-related assets are accessed only by authorized

parties. That is, only those who should have access to something will actually get that access. Confidentiality is sometimes called secrecy or privacy. Integrity means that assets can be modified only by authorized parties or only in authorized ways. Availability means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects that access should not be prevented [4].

The process of encryption and decryption the message in this paper is more like symmetrical algorithm scheme as shown in Figure 1 where:

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input. **Encryption Algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext. **Secret Key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.

The exact substitutions and transformations performed by the algorithm depend on the key. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. **Decryption Algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext [1].

In other word, encryption algorithms encipher the Plaintext, or clear messages, into unintelligible cipher text or cryptograms using a key. A deciphering algorithm is used for decryption or decipherment in order to restore the original information. In general, the enciphering and deciphering keys need not be identical.

Eavesdropping is the interception of messages by a third party monitoring a Communication channel. Anyone trying to break (solve) a cipher is called a cryptanalyst [5].

Cryptanalysis: the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Brute-Force Attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success [1].

The word steganography, with origin in Greek, means "covered writing", in contrast with cryptography, which means "secret writing". Cryptography means concealing the contents of a message by enciphering; steganography means concealing the message itself by covering it with something else [2].

In this paper a new symmetric cryptography algorithm is proposes, which is combine substitution and transposition technique. The substitution technique is mapping each letter into one color in an image (RGB image) and this method to enhance the security by confuses the attacker.

The organization of the paper is divided into sections where section 2 will review the related work. Section 3 gives the details of the algorithm process. Section 4 gives the propose encryption and decryption algorithms. Section 5 will provide the result. Section 6 cryptanalysis discussion and Section 7 conclusion.

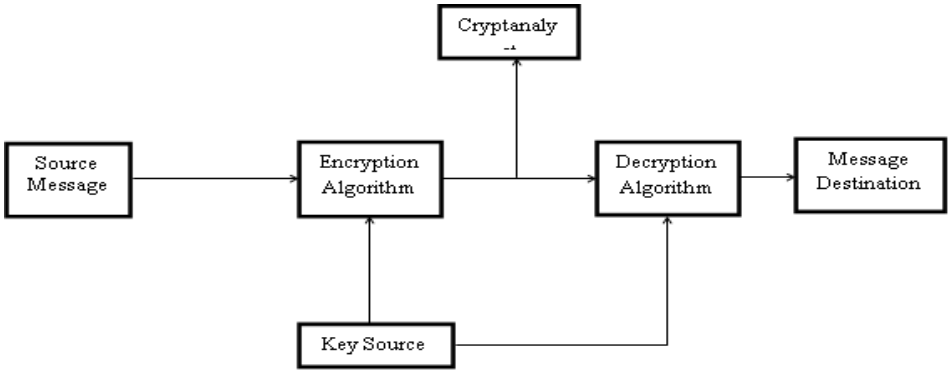

Figure 1: General Symmetric Cryptography Scheme

RELATED WORK

Ahmad Abusukhon, et al. [6] propose new encryption algorithm by encrypt a given text into an image named Text-to-Image Encryption (TTIE). This algorithm consists of two random keys which must share between the sender and the receiver; the keys are long depending on the plaintext length and the number of swapping.

Prof. K. Ravindra Babu, et al. [7] propose new substitution algorithm where the plaintext is substituted with a color block form the available 18 Deucalion's of colors in the world, the algorithm named Play Color Cipher (PCC). Each character from the plaintext will be map into four colors in one pixel, where the size of the result cipher image will be more than the original plaintext four times.

Vishwagupta, et al. [8] propose an advance cryptography algorithm for improving data security. This algorithm essentially based on combination of XOR operation and circular shift between the 16 character blocks.

M. Kiran Kumar, et al. [3] proposes a new encryption algorithm based on matrix scrambling technique. In this algorithm key file will be generated to store the random keys for decryption procedure within define structure which is large in size depending of the plaintext length.

Quist-AphetsiKester, MIEEE [9] propose an image encryption based on RGB pixel transposition and shuffling. In this algorithm no need for any key value, the algorithm based on vectors combination and transpose matrix. In other word if the attacker know the nature of the algorithm the ciphertext will be disclose.

S. G. Srikantaswamy, et al. [10] proposes substitution algorithm based on arithmetic and logic operation. This algorithm read the plaintext and key value, from the key value a set of 6 keys will generated, each character will be added to one of the key set, the result will shifted and complement with the one complement operation, the result will be the ciphertext. Our propose algorithm will used the addition with modular operation to change the original color without using logic operation.

THE PROPOSE ALGORITHM PROCESS

As shown in figure 2, the first block of the algorithm is to initialize index and map arrays for the cipher image which is PNG image format. PNG stands for Portable Network Graphics. It can handle a color depth of up to 48 bits (3 color channels of 16 bits each). It allows you to have different levels of transparency for each pixel (alpha channel). It is a recommended format for digital photography. PNG gives you better image quality at the expense of larger files sizes mainly due to the lossless format used [11]. The maximum map size is 256 × 3, where each level express one color red, green, and blue. The initialization of the map is creating a matrix with zeros in all elements, and the index matrix content sequential values from 1 to 256 to identify which color map will represent each pixel.

The second block for is simply convert each character to a number based on the position of that character in a predefined variable, which is consists of the sequence of characters that may appear in the plaintext. The predefined variable named as alpha.

The substitution method can be defined as:

$$c = (p\ operation\ k)\ mod\ al$$

Where c is the cipher, p is the plaintext, k is the input key, and operation is the operation key value, which is addition or substation, al is the length of the variable alpha. The transposition method is based on discrete logarithms. Briefly, we can define the discrete logarithm in the following way; first, we define (a) as a primitive root of prime number (p), whose powers modulo p generate all the integers from 1 to p-1. Those, if (a) is a primitive root of the prime number (p), then the numbers (a mod p, a^2 mod p,..., a^{p1} mod p) are distinct and consist of the integers from 1 through p-1 in some permutation [1]. The maximum color map of the PNG image is 256 ×3, the prime number chosen is 267 and the primitive root is 3, 5 or 7, in this algorithm 5 is chosen. The transposition method *firstly*; read the X key, Y key and Z key. *Secondly*; the algorithm will find the position of the cipher in the map matrix where the first character will be in X axis, the second character in Y axis and the third character in the Z axis and so on. The position of the character can be express as follow:

$$c1 = 5^X mod\ 257$$

$$c2 = 5^Y mod\ 257$$

$$c3 = 5^Z\ mod\ 257$$

Where c1, c2, c3 are the position of the first, second and third characters, 5 is the primitive root, X, Y, Z are the input keys, and 257 is the prime number.

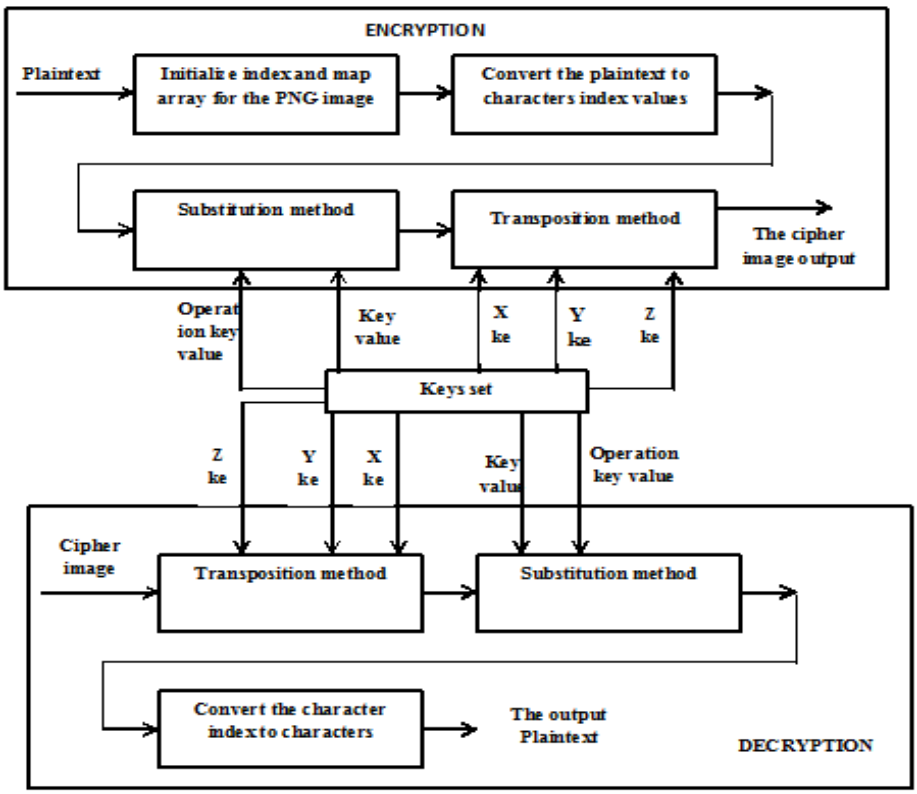

Figure 2: The Propose Algorithm Process Block Diagram

THE PROPOSE ALGORITHM

TIET Encryption

Step 1: initialization of variables

Step 2: Read the plaintext file, operation key, substitution key, X key, Y key and Z key.

Step 3: Convert the plaintext characters to index values.

Step 4: Apply Substitution algorithm on the index values.

Step 5: Apply transposition algorithm on the result of the above step.

Step 6: Write the PNG Image.

TIET Decryption

Step 1: initialization of variables

Step 2: Read the PNG image, operation key, substitution key, X key, Y key and Z key.

Step 3: Apply transposition algorithm on the image pixel values to find the sequence of plaintext characters.

Step 4: Apply Substitution algorithm on the result of the above step to produce the characters index values.

Step 5: Write the plaintext.

EXPERIMENTAL RESULTS

The simulation of this work is carried by MATLAB program as MATLAB m files.

The first experiment:

The plaintext = "Beginning where other security books leave off, Network Security

Architectures shows you how the various technologies that make up a security system can be used together to improve your networks security. The technologies and best practices you'll find within are not restricted to a single vendor but broadly apply to virtually any network system. This book discusses the whys and how's of security, from threats and counter measures to how to set up your security policy to mesh with your network architecture. After learning detailed security best practices covering everything from Layer 2 security to e-commerce design." [12].

The operation key = "-", substitution key = "123", X key = "10", Y key="23", Z key ="12", the prime number = "257" and the primitive root ="5".

The output cipher image show in figure 3.

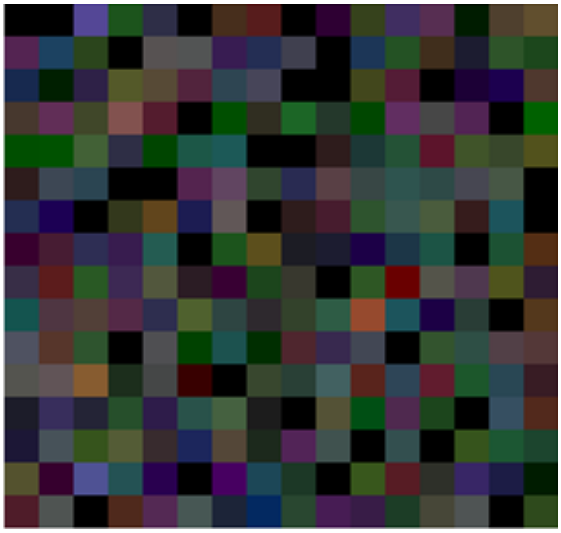

Figure 3: Cipher Image of the First Experiment

The Second Experiment

The plaintext ="This increase in attacks coincides with an increased use of the Internet and with increases in the complexity of protocols, applications, and the Internet itself. Critical infrastructures increasingly rely on the Internet for operations. Individual users rely on the security of the Internet, email, the Web, and Web-based applications to a greater extent than ever. Thus, a wide range of technologies and tools are needed to counter the growing threat. William Stallings NOV 16, 2005." [1].

The operation key = "+", substitution key = "98", X key = "110", Y key="183", Z key ="67", the prime number = "257" and the primitive root ="5".

The output cipher image show in (figure 4).

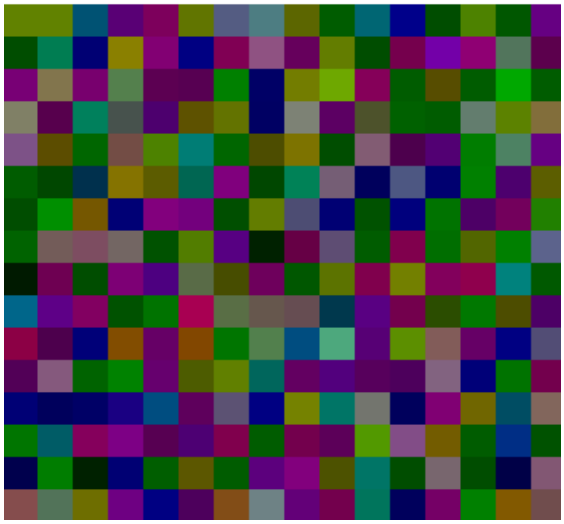

Figure 4: Cipher Image of the Second Experiment

The Third Experiment

The plaintext =It is worth noting that in the existing wired environment, little port security had been implemented, and the internal network was rather wide open to sniffing and other attacks that emanated from within the campus network. Clearly, the security teams concern over wireless illustrated how they judged the new technology by a double standard because the existing environment was not being held to the same scrutiny. But regardless of the policy enforcement

inconsistency, the Security Operations (SECOPS) team still desired to do its utmost to address the perceived wireless vulnerabilities. Unraveling the situation a little more. (see Figure 1). 9-2013" [12].

The operation key = "+", substitution key = "198", X key = "111", Y key="18", Z key ="107", the prime number = "257" and the primitive root ="5".

The output cipher image show in (figure 5).

The decryption in both experiments will produce the same plaintext, after given the same key set.

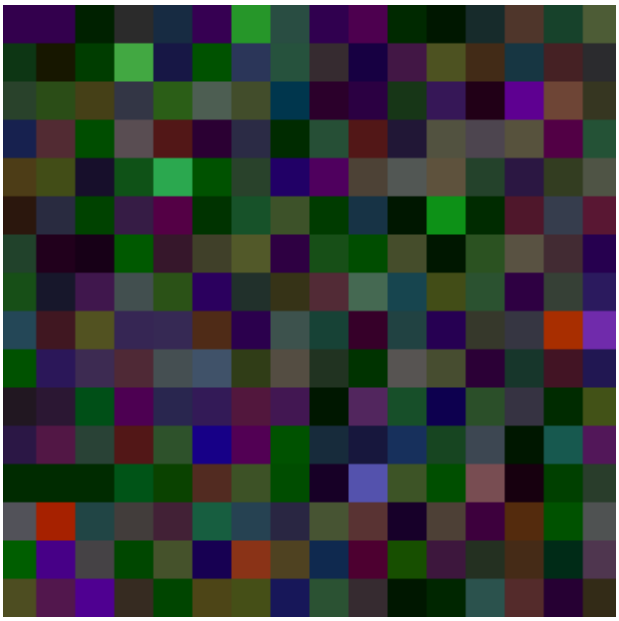

Figure 5: Cipher Image of the Third Experiment

CRYPTANALYSIS

In this algorithm the transformation from plaintext to ciphertext is based on substitution and transposition methods. The results will be converted into cipher image. Five independent keys are used in this algorithm. If the attacker know the nature of the encryption algorithm then all possible keys value must be trying until an intelligible result appears for the attacker. However operation key is two possible value addition or subtraction, substitution key, X key, Y key and Z key have the range from 0 to 256, the possibility for all key will be (256 × 256 × 256 × 256 × 2) which is huge number, this is the case of brute force attack.

If the attacker knows pairs of plaintext and ciphertext values which are the case of cryptanalysis, then the attacker must find the location of each character in the ciphertext with a probability of (256 × 256 × 256).

CONCLUSIONS

With the emergent demands of information security on sending/receiving information in secure way, Therefore number of security algorithm are proposed for information security under the field of network security. Most encryption algorithms known by the attackers so that should be developed continuously.

In this algorithm the plaintext characters will be map into image pixels in different positions in the RGB map. TIET proposes substitution and transposition methods, the substitution method will change the value or the intensity of the color for each character, where the transposition method will re-position the color value in the 3D RGB matrix, finally the transformation to PNG image to confuse the attacker.

REFERENCES

1. William Stallings,"*Cryptography and Network Security Principles and Practices*", 4th edition, Prentice Hall, 2005.
2. Behrouz A. Forouzan, *"Cryptography & Network Security*", Tata McGraw-Hill, 2008.
3. M. Kiran Kumar, S. MukthyarAzam, ShaikRasool, *"EFFICIENT DIGITAL ENCRYPTION ALGORITHM BASED ON MATRIX SCRAMBLING TECHNIQUE*", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.
4. Charles P. Pfleeger- Pfleeger Consulting Group, Shari Lawrence Pfleeger, "*Security in Computing",* 4th edition, Prentice Hall, 2006.
5. KallamRavindraBabu, Dr. S. Udaya Kumar, Dr. A. VinayaBabu,"*A Survey on Cryptography and Steganography Methods for Information Security*", International Journal of Computer Applications, Volume 12– No.2, November 2010.
6. Ahmad Abusukhon, Ahmad Abusukhon, IssaOttoum, *"Secure Network Communication Based on Text-to-Image Encryption*", 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).
7. Prof. K. RavindraBabu, Dr S.Udaya Kumar, Dr. A.VinayaBabu and Dr. Thirupathi Reddy, "*A Block Cipher Generation using Color Substitution* ", International Journal of Computer Applications, 2010.
8. Vishwagupta, Gajendra Singh Ravindra Gupta, "*Advance cryptography algorithm for improving data security*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.
9. Quist-AphetsiKester, MIEEE,"*Image Encryption based on the RGB PIXEL Transposition and Shuffling*", I. J. Computer Network and Information Security, 2013, 7, 43-50.
10. S. G. Srikantaswamy, Prof. H. D. Phaneendra, "*A Cipher Design using the Combined Effect of Arithmetic and Logic Operations with Substitutions and Transposition Techniques*", International Journal of Computer Applications (0975 – 8887) Volume 29– No.8, September 2011.
11. Sebastian Montabone, "*Beginning Digital Image Processing*", APRESS, 2010.
12. Sean Convery, "*Network Security Architectures*", Cisco Press, 2004