IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. I (Jan – Feb. 2015), PP 07-13
www.iosrjournals.org

A Novel Method of Generating (Stream Cipher) Keys for Secure Communication

[1]Zainalabideen Abdullasamd Rasheed, [2]Ali Abdul Azeez Mohammad Baker
(Education college/Kufa University/Iraq)

Abstract: *Security is an important part of computer science that deals with the protection of important information from access, change or modified, and delete, so there are many ways to improve the security of information like cryptography, steganography, biometrics, passwords, barcode….. However most of these methods are considered keys required.These keys are used to implement the changing of the information for secure style purpose. For that reason, generating and keeping these keys is a major part of the appropriate security system. Moreover, sending the key to the wanted person in unsacred channel is a widely weakness part for any system. The proposed system is a novel method for generating a secret unique key from an image. A generating process is applied by discovering the essential colors in the image and constructing a table values for these essential colors , after that a suitable threshold is used to considered these values are (0, 1) bits which will be used as stream bits key.*

Keywords: *stream cipher, secret key, x-or, ciphering, security.*

I. Introduction

Encryption algorithms are concerned of transforming readable texts (plaintext) to unreadable and uncomprehending text (ciphertext). In stream ciphers, the encryption algorithm generates a stream of bits that are exclusively-OR with a stream of plaintext bits to generate a stream of ciphertext bits.

Traditionally, stream ciphers use textual secret key to initiate the key generation process. The textual secret key is used as Initial Vector in all stream ciphers. For security purposes, these keys should be long enough to satisfy the minimum security requirements.

The idea of stream ciphers was derived from the famous cipher called the One-time Pad. This cipher is based on applying XOR ($\oplus$) gate between the message bits and the key bits. The One-time pad is defined in **Equation1:**

$$E :\{ 0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}, (m, k) \rightarrow m \oplus k \quad \dots (1)$$

Where plaintext, key stream and ciphertext bits are in the space {0, 1}. The encryption Function is given by:

$$E_{ki} (m_i) = m_i \oplus k_i = c_i \in C \quad \dots (2)$$

And the decryption function is given by:

$$D_{ki} (c_i) = c_i \oplus k_i = m_i \in M \quad \dots (3)$$

The most important step in stream cipher security is the security of the key and the strength of any stream cipher method depends on the strength of the key.

The general structure of stream ciphers can be illustrated in figure (1).

Many stream ciphers have been proposed over the past 20 years. Most of them are constructed using a linear feedback shift register (LFSR), which is easilyimplemented in hardware, but the software implementations are mostly slow. In recent years, several word-oriented stream ciphers have been proposed and standardized. The idea of a stream cipher is partition the text into small blocks (e.g. 1bit), the encoding of each block depends on the previous blocks, and the different keys are generatedfor each block. While the idea of a block cipher is partition the text into large blocks (e.g. 128bit), the encoding of each block independently, and the same key is used for each block.

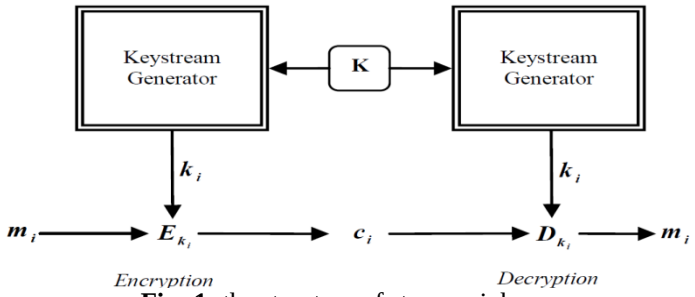


Fig -1: the structure of stream ciphers

II. The Proposed System

The proposed system consist of key stream constructing method in addition to two stages the first one for encryption text while the another one for decryption text as illustrated in figure (2), (3), (4)

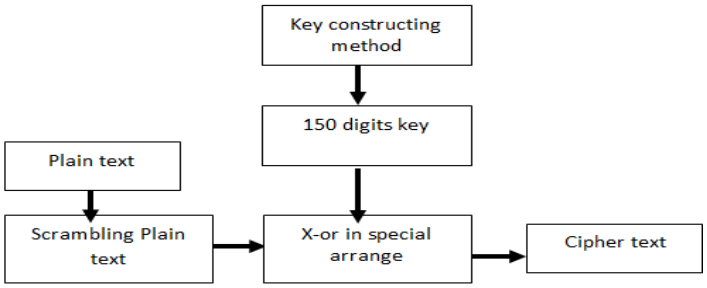


Fig -2: Block diagram of ciphering method

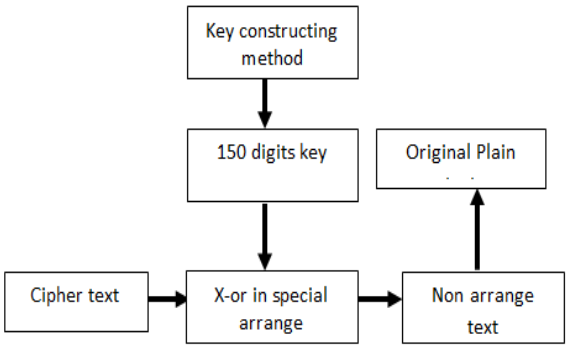


Fig -3: Block diagram of deciphering method

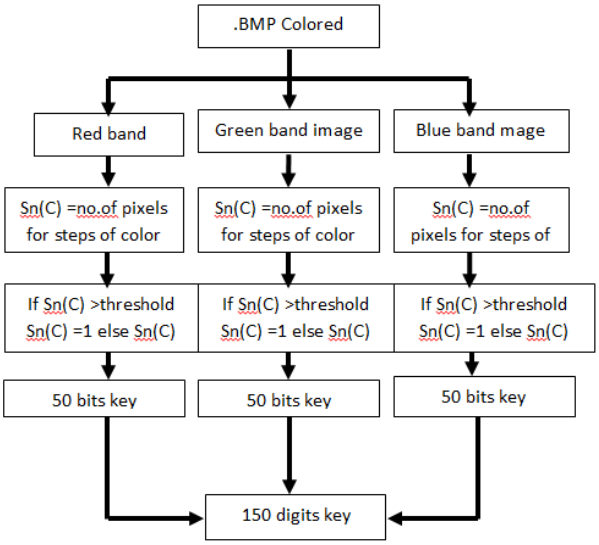
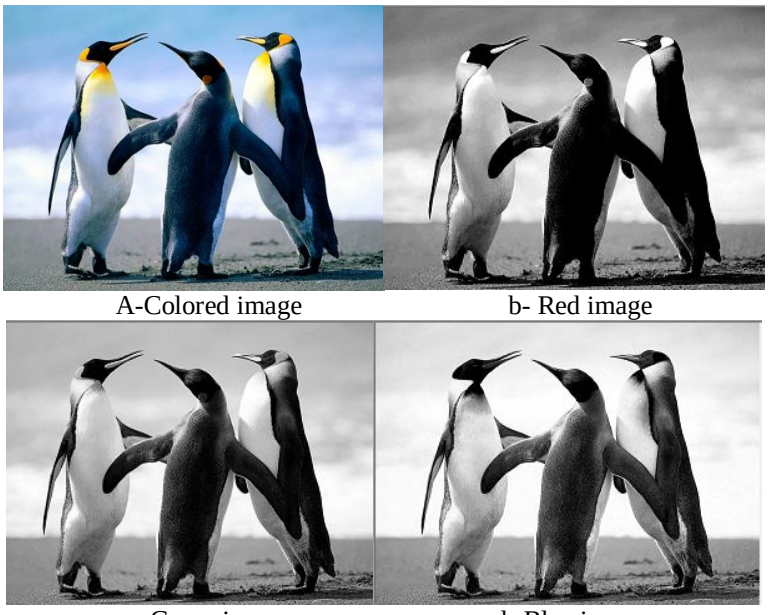


Fig -4: Block diagram of key constructing method

a. key constructing: The steps of the proposed method for key constructing can be illustrated by the following explaining

1- Separate colored image into three gray scales images.
2- Calculate the array Sn(c) for each gray scale imagewhere $1 \leq c \leq 50$ which is represent integer number of pixels in each step of five colors in the image except first step (0→10).
3- Calculate the threshold that is (0.01 × Image width × Image height).
4- For each Sn(c) greater than the threshold put bit (1) in the corresponding position of the key, and for each Sn(c) smallest than the threshold put bit (0) in the corresponding position of the key.
5- Merge the fifteen bits for each band to construct 150 bits key.

The following example for image illustrated in figure (5) will be explained the above steps



A-Colored image b- Red image

c- Green image d- Blue image

Fig -5: Example image

The number of pixels in each step can be illustrated in figure (6)

This images with dimensions of (307×230) pixels, so the threshold equal round (0.01 × 307 × 230) = 706

Then each step with value greater than 706 become one and the others become zero as illustrated in figure (7)

	s(1)	s(2)	s(3)	s(4)	s(5)	s(6)	s(7)	s(8)	s(9)	s(10)	s(11)	s(12)
red image	2288	723	949	1108	1163	1180	1061	1038	993	1009	871	718
green image	5381	1853	1470	1138	886	691	710	636	576	555	527	463
blue image	13383	571	480	412	383	299	315	297	314	337	334	358

Fig -6: number of pixels in each step

	s(1)	s(2)	s(3)	s(4)	s(5)	s(6)	s(7)	s(8)	s(9)	s(10)	s(11)	s(12)
red image	1	0	0	0	0	0	0	0	0	0	0	0
green image	1	1	1	0	0	0	0	0	0	0	0	0
blue image	1	0	0	0	0	0	0	0	0	0	0	0

Fig -7: (50) bits key for each band

b. cipher algorithm: The steps of the proposed method for cipher algorithm can be illustrated by the following explaining

1- Translate the message to binary representation.
2- Construct square array with dimension (10 × 10).
3- Apply a transform to scramble plaintext then translate the scrambling array into vector.
4- Apply X-or with bit (i) from the plain text with all bits of the key less than or equal to (i).
5- Save the first 100 bits of ciphertext and return points (1→5) until message ending.

The above steps can be explained by the following example

Plain text is:
UNIVERSITY OF KUFA EDUCATION COLLEGE

ASCII representation is:
85 78 73 86 69 82 83 73 84 89 79 70 75 85 70 65 69 68 85 67 65 84 73 79 78 67 79 76 76 69 71 69.
Binary representation of plain text is:
1010101 1001110 1001001 1010110 1000101 1010010 1010011 1001001 1010100 1011001 1001111 1000110 1001011 1010101 1000110 1000001 1000101 1000100 1010101 1000011 1000001 1010100 1001001 1001111 1001110 1000011 1001111 1001100 1001100 1000101 1000111 1000101

The first square array is
$$\begin{bmatrix} 1&0&1&0&1&0&1&1&0&0\\ 1&1&1&0&1&0&0&1&0&0\\ 1&1&0&1&0&1&1&0&1&0\\ 0&0&1&0&1&1&0&1&0&0\\ 1&0&1&0&1&0&0&1&1&1\\ 0&0&1&0&0&1&1&0&1&0\\ 1&0&0&1&0&1&1&0&0&1\\ 1&0&0&1&1&1&1&1&0&0\\ 0&1&1&0&1&0&0&1&0&1\\ 1&1&0&1&0&1&0&1&1&0 \end{bmatrix}$$

The transform can be explained by the array
$$\begin{bmatrix} 1&1&1&0&1&0&1&1&0&1\\ 0&1&1&0&0&0&0&0&1&1\\ 1&1&0&1&1&1&0&0&1&0\\ 0&0&1&0&0&0&1&1&0&1\\ 1&1&0&1&1&0&0&1&1&0\\ 0&0&1&1&0&1&1&1&0&1\\ 1&0&1&0&0&1&1&1&0&0\\ 1&1&0&1&1&0&0&1&1&1\\ 0&0&1&0&1&1&0&0&0&1\\ 0&0&0&0&1&0&1&0&1&0 \end{bmatrix}$$

and the vector become:
11101011010110000011110111001000100011011101100110001101110110100111001101100111001011000100000101010000011010100100011111011010001111011000101000001100010000011100110101011000011101001110010100101100011110111111100111111110000111111111011111111101111111110111111111011111111101111111111111111111111111111111

The key is:
11111011011011010011010010010010010000000000000000000000000000011011011111111111111111111111111111111111111011011011011011011011111111011011111111111111111111
1 ⊕ 1=0
1 ⊕ (1⊕ 1) =1
1⊕ (1⊕1⊕ 1) =0
0⊕ (1⊕1⊕ 1⊕1) =0
1⊕ (1⊕1⊕ 1⊕1⊕1) =0
0⊕ (1⊕1⊕ 1⊕1⊕1⊕0) =1
1⊕ (1⊕1⊕ 1⊕1⊕1⊕0⊕1) =1
1⊕ (1⊕1⊕ 1⊕1⊕1⊕0⊕1⊕1) =0

And so on for next positions then **cipher text become**:
01000110111011100001101011010100111100100010011001110010001001111100011000110010011110010001010111111101110111001001110011011110111010011011111010110010010101010100000110100011011001111111010110100111000010000000110100100110110101010001010101110101010111001001000001001001001010101110101010101110101010

c. Decipher algorithm: The steps of the proposed method for decipher algorithm are the same for cipher algorithm but in reverse fashion.

III. Results

The proposed system will be applied on some messages and images; we can show the following results

Example 1:

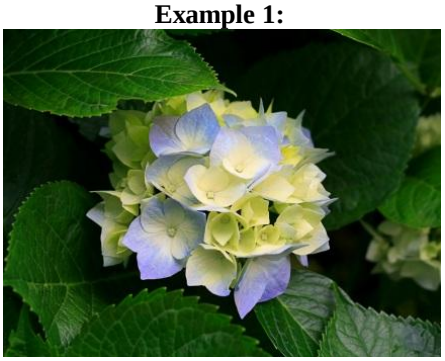


Fig -8: example (1) of the proposed system

binary representation of plain text:

1000001100110010010011000001100001010001001010101100110010000011011010100010110001011011010100110110011111100100010000011001101100110110000011000100100000101000001100101110001011010010101000110000011011010101101010000011011010111111111111111111111111111111111111111111111111111111111111111111111111111111111

Secrete key:

1111111111111111111111111111111111110110111111111111100101100100100100100100100100000100100000100100100100100100100110100100000000000000000000000000000000

Cipher text:

1010000111000011100110100011101110111011110110100110101100000111110110111111010110011000001111111111010001000100000011000101000010000100010010000010110001101000001101101000100111111101010110101010000011000100110100100111000101000111000000111011000111000101000111010111011010111111111100111111110011111111

Example 2:

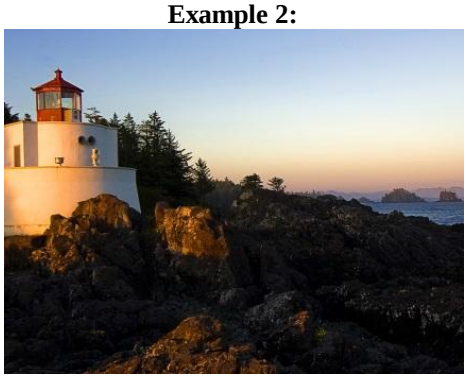


Fig -9: example (2) of the proposed system

Binary representation of plain text:

1011010110000111010011101110110000111011001100001110001011010011100100110010111001011101110010000010000011100010110010011101011101100110110011000011110011110000111011011100100010000010100101100001111001111010001100101110010111001001111111111111111111111111111111111111111111111111111111111111111111111111111111111

Secrete key:

1111111111111111111110110100000000000000000000000010000000000000000000000000000101101101001011011011011011011011011011011111111111111111111111111111111001001

Cipher text:
0000111110100010110001110010011100101010011101111000001111011100101011001110001000101010010111010110111010000000001111010001001011001000010111001010110111001100101011000001010110110000101001011010101000110000000000000000001100000011111011000110110110101110110110100110101111101010111010101011011000111

Example3:

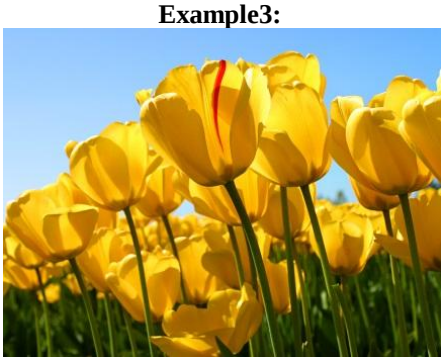


Fig -10: example (3) of the proposed system

Plain text:
I want to publish my search fast as possible as can

Binary representation of plain text:
1001001111011111000011101110111010011101001101111111000011101011100010110110011010011110011110100011011011111001111001111001011100001111001011000111101000110011011000011110011111010011000011110011111000011011111110011111001111010011100010110110011001011100001111001111000111000011101110111111111111

Secrete key:
1001011011011011111111111111011011011010010010010010010010010010011011011011011011011011011011011011011011011011011011011011011011011011

Cipher text:
0101001101001011111111010001000111110110100000000101000000010011001001111100001001110100000000111000100010000110001000100011100100010001110001110010001101001111001000011000010111111011000001011100110110010100111010100110001011001011101100100001011110001011011100001011011111001111001100110001000010100110 0

IV. Conclusions

1- Generating keys from an image is a powerful method for sending secret key with less probability of discovering the critical information.
2- In term of channel noise or compression could be happen to the image our proposal has been proved that even this modification happen to the image the key is still able to construct because depend on the essential colours iteration in image which is less effected by noise or compression algorithms.
3- A stream key bits cipher construct is based on suitable threshold which determine the bits value, this threshold is also depend on size and number of iteration of each colours in image. That is means as long as this threshold be bigger the key bits cipher will be more robust against loss compression or noise.
4- In addition, the two parties can extract the secret key from same downloaded image from the internet for more safety against channel modification.

Referances

[1]. Ali Abdul Azeez Mohammad Baker, ZainalabideenAbdullasamdRasheed" Secure Keys Constructing", Education College, Kufa University, International Journal of Advanced Research in Computer Science and Software Engineering ,2014, Iraq.
[2]. NesirRasoolMahmood, Ali Abdul Azeez Mohammad baker, ZahraaNesirRasool " Public Key Steganography", Kufa University ,Education College, International Journal of Computer Applications,2014, Iraq.
[3]. Abhishek Roy, Sunil Karforma" STREAM CIPHER BASED USER AUTHENTI-CATION TECHNIQUE IN E-GOVERNANCE TRANSACTIONS", Journal of Research in Electrical and Electronics Engineering, 2014, INDIA.
[4]. PratishDatta, Dibyendu Roy and SouravMukhopadhyay "A Probabilistic Algebraic Attack on the Grain Family of Stream Ciphers", India.
[5]. Xinxin Fan and Guang Gong "Specification of the Stream Cipher WG-16 Based Confidentiality and Integrity Algorithms", 2012, CANADA.

[6]. KHALED SUWAIS " Parallel Model for Rabbit Stream Cipher over Multi-core Processors", WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, 2014, SAUDI ARABIA.
[7]. Jing Lv,Bin Zhang, and Dongdai Lin" Some New Weaknesses in the RC4 Stream Cipher", Springer International Publishing Switzerland 2014, china.
[8]. Ruben Niederhagen "Stream Ciphers and Block Ciphers" September 18th, 2013, Eindhoven University of technology.

.

About Authors

Zainalabideen Abdullasamd Rasheed University of kufa, Education of College, Najaf /Iraq. Has a BSc (Baghdad University, Iraq), and MSc (Buckingham university, United).he has a long experience in teaching various computing practical courses at Baghdad university .at AL Kufa university, MrRasheed teaches different courses like computer organization, operating system and computer architecture .he supervises undergraduate projects. He interest in data security (steganography and cryptography) and digital image processing (biomedical image and edge detection, de-noising images).E-mail: zain9999@live.com, Tel: 009647711131246 .Iraq.

Ali AdulAzeez Mohammad Baker University of Kufa, Education College, Najaf, IRAQ. He received BSc in computer sciences (2010), civil engineering (1990), and MSc in computer sciences (2012), worked as a teacher in Kufa University, has many published papers. His research interests are in image processing, and security (biometrics, and steganography), He's Associate teacher in Computer Science at the University of Kufa – Najaf, IRAQ. E-mail: alia.qazzaz@uokufa.edu.iq, Tel: +964-7803369309.