Journal of Computer Networks, Architecture and High Performance Computing
e-ISSN 2655-9102, Volume 2, No. 2, july 2020, pp 237-244

Implementation Gifford Method For Digital Image Security

Fauduziduhu Laia[1], Erwin Panggabean[2]

[1,2]Informatics Engineering Study Program, STMIK Pelita Nusantara, Jl. Iskandar Muda No. 1 Medan, North Sumatra, Indonesia 20154

E-mail: fauduziduhulaia@gmail.com

Abstract-*Rapid development of digital image technology secret causes images require security aspect. Reviews These digital secret image can be encrypted using cryptographic methods. After being encrypted, the image is randomized, so that if it is Obtained by an unauthorized party, the image has no meaning. The cryptographic algorithm used in this study is Gifford method. The Gifford method is a stream cipher, a symmetry encryption algorithm that transforms the data character by character. Gifford has 8 registers filled with key bits. The processes performed by the Gifford method are the Output Function process, the 1-bit Sticky Shift Right process, the 1-bit Left Shift process, the XOR operation and the shift register operation to the right. The decryption process must use the same key as the encryption process in order to Obtain the original image.*

Keywords *: Encryption, pixel color, Gifford*

1. Introduction

Imagery is usually used to store information in the form of images. Digital imagery has been widely used in various fields of human life, including the medical, research, business, military and other fields. In some cases, digital images are used to document things that are confidential, so that the image can only be accessed by certain people only. Examples of the image containing confidential information is the image of the project design, building, office complex and the work in the world of civil engineering (Tempo.co, 2014). The owners do not want the image of the design is stolen and can be accessed by competitors. The other areas that require security is an image in the field of business, such as product design secrets to a company, the image of a patient's medical diagnosis in the medical field, the image of secret documents in the intelligence field, to the private image created for personal documentation (Madhu, et.al, 2016). Confidential so that the image is not accessible to everyone, then the digital image can be encrypted using cryptographic methods. Once encrypted, images become scrambled, so that even if acquired by an unauthorized person, the image has no meaning. To restore the image to its original shape, so do the decryption process by using a specific keyword. Thus, only certain parties can access the image. Gifford method is one of the cryptographic algorithm that can be used to secure the digital image. This method was developed by David Gifford. In the science of cryptography, Gifford is a stream cipher method, namely symmetric encryption algorithm that transforms data character by character (byte by byte). Stream ciphers can be made very quickly, much faster than that of any block cipher algorithm. Gifford method has 8 registers, namely: b0, b1, b2, b3, b4, b5, b6 and b7. These registers have a value that is filled with the bits of the key before further processing. The processes performed in the Gifford method is the process Output Function, Shift Right Sticky process one bit, the Left Shift 1 bit, XOR operation and sliding operation of the register to the right. Therefore Gifford is a symmetric key cryptography, the decryption process must use the same key to the encryption process, in order to obtain the original image. Based on the description in the background, it will develop an application that can do security on the digital image, through the encryption and decryption process using the Gifford. Thus, this thesis is entitled "Implementation of Gifford Method for Digital Image Security".

2. Theory

2.1. Cryptography

The word cryptography (cryptographic) is derived from the Greek, meaning that KRIPTOS secret (secret), and graphein, which means writing (writing). So, the secret cryptographic means writing (hieroglyph).There issome definitions of cryptography that has been presented in the literature. The definition used in the books of the old (before the 1980s) states that cryptography is the science and art to maintain the confidentiality of messages by way of encoding it into a form that can no longer understand the meaning. This definition may be suitable in the past where cryptography is used for safety critical communications such as communication

among the military, diplomats and spies. But nowadays cryptography is more than just privacy, but also for the purposes of data integrity, authentication and non-repudiation. (Mollin, 2010)

In his book entitled "Handbook of Applied Cryptografphy ', Alfred Menezes, Paul van Oorschot and Scott A. Vanstone (1996: 4) defines cryptography as the study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity and authentication. While Bruce Schneier (2016: 1) in his book "Applied Cryptography", defines cryptography as a science and an art to maintain the security of the message.

Cryptography is the science and art to keep your messages. Security is obtained by encrypting messages into messages that do not mempuyai meaning. Today, the confidentiality of information into something important. Confidential information that needs to be hidden so as not known by people who are not eligible. Someone certainly do not want a credit card or a PIN number of his ATM card known. Or, if a message written in secret and does not want to know or read by others. Cryptography can be used to disguise the confidential information of the person or party who is not entitled to read it. (Munir, 2012: 203)

2.2. Gifford

David Gifford find a stream cipher used to encrypt mail and cable (wire news report) in Boston. In cryptography, Gifford is a stream cipher, the symmetric encryption algorithm that transforms data character by character. This method has an 8-byte register, namely: b0, b1, b2, b3, b4, b5, b6 and b7. These registers have values or initial conditions before the subsequent processing (Schneier, 2016).

2.3. Key Generation Process Gifford

This process must be done to generate key bits to be used in the encryption and decryption process. The processes performed in the Gifford methods generate key bits is as follows,

1. Process 1: Process Output Function.
   *output*of this process is random along the 8 bits. To generate a random number, perform the merging operation (concatenate) between registers b0 and b2 registers and between registers and registers b4 b7. Then, perform a multiplication operation between the result of the merger to produce a 32-bit number. Byte third from left is the output of random numbers. Output process function can be seen in Figure 1.

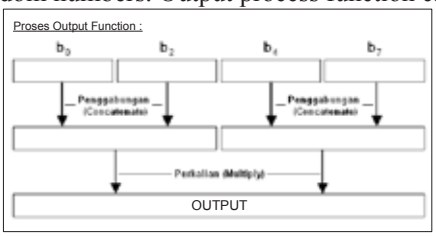

Fig 1. Work Procedures Asymmetric Algorithm

2. Process 2: Sticky Shift Right 1 bit to register b1.
   Take the contents of registers b1 and do the process right shift 1 bit sticky to b1. This means shifting bits (shift) to the right. Rated left most bit is maintained and vacant shifted bits (bits that are behind the left most bit) is replaced with the value left most bits. The result is stored to the variable A.
3. Process 3: Left Shift 1 bit face to register b7.
   Take the contents of the register b7 and do surgery left shift one bit. This means that all the bits shifted (shift) to the left and right most bit value is filled with value 0. The result is stored to the variable B.
4. Process 4: XOR operation to register b0, the value of the variable A and the value of the variable B
   Perform XOR operation of the contents of the register b0, the value of the variable A (the result of the second process) and the value of the variable B (the result of the third process). This means that the operation will generate a bit value of '0' (zero) for the bits of the same value and will generate a bit value of '1' (one) for the different bits .Hasilnya stored to the variable C.
5. Process 5: Slide blocks register b to the right one block
   Scroll register b (b0 ... b7) 1 block to the right. This means that the register b7 removed (discard), register b6 filled by registers b5, register b5 filled by registers b4, register b4 filled by the register b3, register b3 filled by the register b2 and register b2 filled by the register b1, while the register b0 empty, filled by the value of the variable C (the results of the fourth process).

   Gifford bit key generation process can be seen in full in Figure 2.

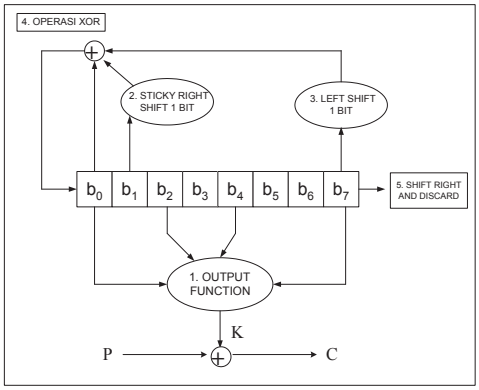

Fig 2. Power Bit Key at Gifford Method

2.4. Encryption and decryption processes Gifford

The encryption process on Gifford method will use the key bits to transform plaintext into ciphertext, and vice versa in the decryption process. Encryption and decryption process is in the form of an XOR operation of plaintext and ciphertext or key to produce the ciphertext and the key XOR operation to generate plaintext (Schneier, 2016).

$$P = C \quad K$$
$$C = P \quad K$$

with:

P= *plaintext*
K = *Key*
C = *ciphertext*

2.5. imagery

Image is a representation (picture), likeness or imitation of an object. Image as the output of a system is an optical data recording can be images, is an analog form of video signals such as images on a TV monitor, or digital nature that can be directly stored on a storage medium. (Sutoyo, et al, 2010: 9)

3. Analysis

The analysis process to discuss the workings of the process of formation of key bits, the encryption process digital images and digital image decryption process by using Gifford.

3.1. Formation Bit Key

For example, if the key used is 'Fauduzid' and about to be raised 10 pieces of sub key, then the key establishment process of the key sub-1 to sub-10 is key to the following:

The initial value of the register b (0) to b (7):

input key = 'Fauduzid'
b (0) = binary (ascii of the letter 'F') = binary (70) = 01.00011 million
b (1) = binary (ascii of the letter 'a') = binary (97) = 01,100,001
b (2) = binary (ascii of the letter 'u') = binary (117) = 01110101
b (3) = binary (ascii of the letter 'd') = binary (100) = 01.1001 million
b (4) = binary (ascii of the letter 'u') = binary (117) = 01110101
b (5) = binary (ascii of the letter 'z') = binary (122) = 01.11101 million
b (6) = binary (ascii of the letter 'i') = binary (105) = 01101001
b (7) = binary (ascii of the letter 'd') = binary (100) = 01.1001 million

Key sub-1

1) *output Function*
   a. Combine the contents of b (0) and b (2), and B (4) and b (7).
      b (0) and b (2) = 0100011001110101
      b (4) and b (7) = 0111010101100100
   b. Multiply the result of merging the register:
      X 0100011001110101 0111010101100100
      = 00100000010011101111111010110100
   c. The results of the key sub-1 = 11.11111 million (third from left byte)
      = FE (hex)
2) *Sticky shift right* 1 bits in b (1)
   A = SSR (b (1))