International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 6235-6240

A Proposed Method for Generating a Private Key Using Digital Color Image Features

Wisam Abed Shukur

Baghdad University, College of Education for Pure Science/Ibn Al-Haitham, Computer Sci. Dept., Iraq.

Orcid: 0000-0001-5000-5537

Abstract

In this paper, the goal of proposed method is to protect data against different types of attacks by unauthorized parties. The basic idea of proposed method is generating a private key from a specific features of digital color image such as color (Red, Green and Blue); the generating process of private key from colors of digital color image performed via the computing process of color frequencies for blue color of an image then computing the maximum frequency of blue color, multiplying it by its number and adding process will performed to produce a generated key. After that the private key is generated, must be converting it into the binary representation form. The generated key is extracted from blue color of keyed image then we selects a cover that is digital color image for hiding a text in that selected cover for testing a proposed method of generating the private key. The hiding algorithm used is least significant bit (LSB). Finally, the generated key is tested by hiding process and changing the extension of image, after that notice the generated key is not changed or modified. the Matlap language is used to design and implement a proposed method.

Keywords: Private Key, Data Encryption, Digital Iimage, Image Feature.

INTRODUCTION

In our world today, with the open networks to transmit data therefore, the encryption becomes more important for many persons and parties to protect its individual data. There many scientific researches produced in this field to present strong cipher methods then increasing security of data. Since the encryption is the science that use mathematics foundations to encrypt and decrypt data, the improvement of encryption methods generally was either via development the foundations of mathematics models for encryption or development the private and public keys generating process of symmetric and asymmetric cipher methods.

CRYPPTOGRAPHY

Cryptography is the process or skill that transforms information in such a way that no one other than the authorized person can read what was actually written, the cryptography played a major role during world war ıı [1]. The characteristics of cryptographic methods are transformation type, keys number and processing mechanism[2].

The various complex transformations are used by some cryptography methods. These methods uses different operations such as permutations and substitutions processes to produce an encrypted or secret text from the plaintext. There are two types of cryptographic methods, the first type is symmetric key methods that uses the same key in encryption and decryption operations, the second type is asymmetric key or public key methods that uses different keys in encryption and decryption operations and the key used in decryption operation cannot derived from the key used in encryption operation. The popular examples of symmetric key methods are DES and Rijndael algorithms [3], while the popular example of asymmetric key or public key methods is RSA algorithm and its strength comes from the difficulty that is too complex to factor chosen large prime numbers [4]. Basically the manner type of dealing with the plaintext by encryption methods is divided into two manners, the first manner is stream cipher and the second manner is block cipher. These methods are similar excepting the amount of inputted data for each encryption operation at a time in each passing process[5]. The one way ciphering is a special type of cryptography, this type of encryption considered as an irreversible ciphering process.

The secret message or plaintext cannot extracted or recovered from the encrypted text. In UNIX systems, all passwords are encrypted using an irreversible or a one way ciphering algorithm[3].

CRYPTOGRAPHIC KEYS

The various classes of keys are signing keys, authentication keys, session keys, key encryption keys and root keys. the digital signature is created by using the signing keys, for any authentication process between computers and others computers or an individual users and computers, an authentication keys are used for this purpose. For a short time, to encipher a secure channel via the networking environment the session keys are used, for any application wants sending a

key to another, the is ciphered with another key and these keys are called KEK. Finally, the root keys are used for signing all keys that originate from an authoritative source[6]. Generally, the cryptographic algorithms are divided into three classes, the first class is the transformation type from plaintext to cipher text[7]. The second class is the keys used in ciphering and deciphering processes, if ciphering and deciphering processes use the same key then the cryptographic algorithm is called symmetric, while both use the different key the cryptographic algorithm is called asymmetric[8]. The third class is the type of processing for plaintext, the processing type plaintext can be classified into types that are stream and block cipher[9]. there are two types of cryptographic algorithms, the first type is symmetric-key algorithms and the second type is public key algorithms. An algorithms with symmetric key uses the key in a series of rounds. An examples of symmetric-key algorithms are Triple DES and Rijndael(AES)[10]. In public-key algorithms, there two different keys are used for encryption and decryption processes. the second key that used in decryption process cannot be derived from the first key that used in encryption process. RSA is an example on public-key algorithms[11].

STEGANOGHRAPHY

With expending influence of information technology and communications infrastructure, people want to securely communicate among secure parties. New developments in science and technology are helping foster that cause [12]. Thus, information hiding and algorithms employed to protect data become more of interest to individuals and organizations alike [13]. In 1983, Simmons defined a steganography security model as a cryptographic problem. the prisoners' problem represents that model. Where sender(Alice) and receiver (Bob) as prisoners want to communicate for exchanging messages between them, the Warden monitors communicated parties of their correspondence. There are two variation types of problem: active and passive warden [14]. In passive case, the warden is permitted to review only but other actions such as changing or modifying of messages are not permitted; however, the block process of communications and alter privilege levels or otherwise punish both sender and receiver are permitted to the warden as shown in Figure (1).

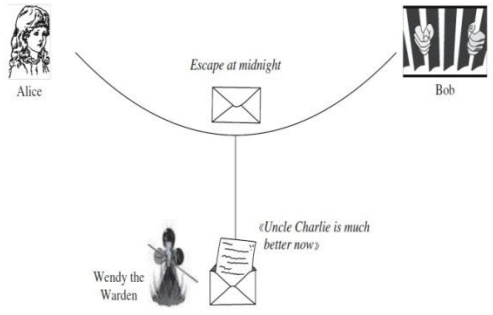

Figure (1): Prisoners' problem with passive warden

In an active case, the warden can modify messages between sender and receiver. There are two actions the warden can take: disabling the hidden message which would amount to DoS attack; and message forging which receiver would believe as genuine message coming from sender.

A steganography security system is considered as a special case of a cipher system where secret message, cover, embedding algorithm, extraction algorithm and optional key interplay [15]. A generic example of stego-system is shown in Figure (2).

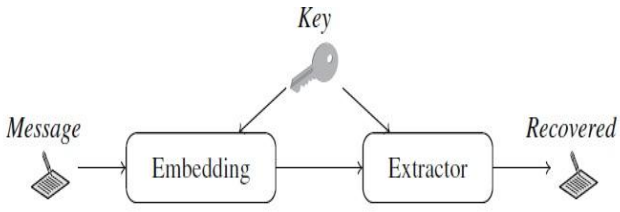

Figure 2: A generic (shared-key) system for steganography using cover synthesis

A stego-system is called as a 'steganography by cover synthesis', where the stego-encoder (embedding/encryption) algorithm synthesizes an innocuous cover that must not be related to the secret message [15]. Stego-systems that perform cover synthesis are few, since cover synthesis is considered as challenging. by taking an innocuous cover, key and the message to be embedded into the cover leads to avoid this challenge with steganography by modification as shown in Figure (3).

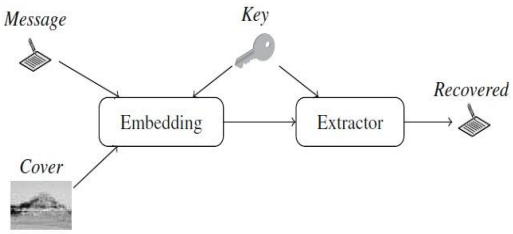

Figure 3: A generic (shared-key) system for steganography by cover modification

THE PROPOSED METHOD

The goal of this proposed method is generating a cryptographic key by using digital color image which has extension JPG via computing number of frequencies for three colors of image that are red, green and blue by using mathematic formula to compute frequencies for each one of them in mathematic manner to construct the general frame for generating process. In this paper, the proposed method includes three basic phases that are initialization phase, generating phase and testing phase. The testing phase has two sub phases that are testing via hiding and testing via

extension. The testing phase is an important in this proposed method to show all changes that possible happen since many factors such as hiding a secret information in image and exchanging an extension of image. finally, is generated key by this proposed method changed or not since that factors. All mathematical calculations of color frequencies for image are applied by generating phase. Each one of these phases performs a specific tasks that helps in process of cryptographic key generating. Using feature of image such as color for generating a cryptographic key to encrypt sensitive information securely. Mathematical calculations of color frequencies for image acts the core or basic idea of proposed method. All of these phases are shown in Figure (4) and will be explained in the next section in details.

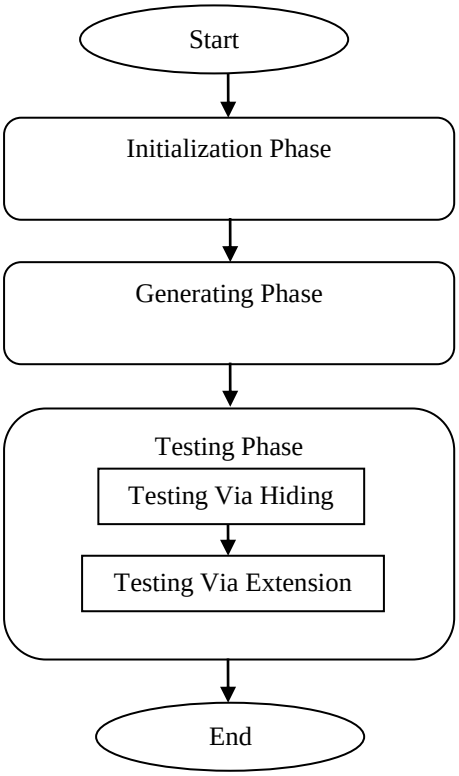

Figure 4: General flowchart of the proposed method

Initialization Phase

This phase is considered as preprocessing process for generating a cryptographic key. In this phase, there are three main steps as shown below:

i. Specify digital color image that used to generate the cryptographic key from its features such as color (red, green and blue) and the specified image must has JPG extension.

ii. Specify an image that used as cover or host for hiding process, the specified cover or host image must be color.

iii. Specify the text that considered as secret information to embed it in a cover or host image that specified in the above step and convert selected text into binary form.

Generating Phase

In this phase, an image that specified in an initialization phase will be loaded and readed. After reading that image, the frequencies of image colors (red, green and blue) for this image will be computed. The (R-fre) represents the number of red frequency in an image, The (G-fre) represents the number of green frequency in an image and The (B-fre) represents the number of blue frequency in an image. The maximum frequency of each color of an image is computed. The (MAX-R) represent the maximum frequency of red color in an image, The (MAX-G) represent the maximum frequency of green color in an image and The (MAX-B) represent the maximum frequency of blue color in an image. For each color of them, the maximum frequency will be multiplied by the number of frequencies. The result of multiplying operation is the cryptographic key that must converting it into binary representation to use in encryption process. The generating of the cryptographic key from digital color image is shown in Figure (5) below:

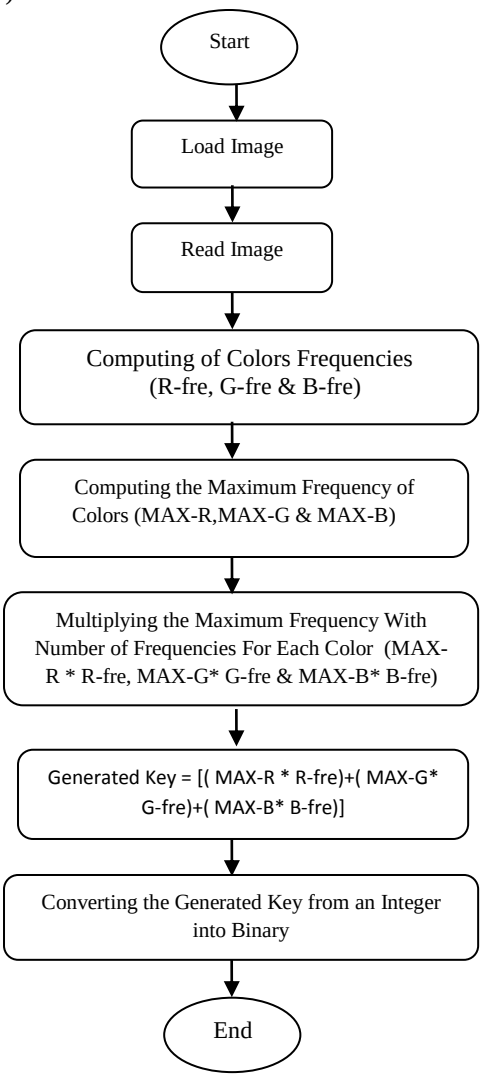

Figure 5: General flowchart of the generating phase

Testing Phase

In this phase, there are two steps for testing as shown below: i- testing via hiding ii- testing via extension. Each one of them will discuss in detail below:

i- Testing via Hiding: the goal is verifying a generated cryptographic key cannot change or modified. this goal performed by using hiding operation. In this work, the specified text in an initialization phase will be hide in an image as cover after applying XORing operation between the generated cryptographic key and text. Finally, recounting colors frequencies of an image after hiding operation to check if the generated cryptographic key is changed or not? This step is shown in Figure (6) below:

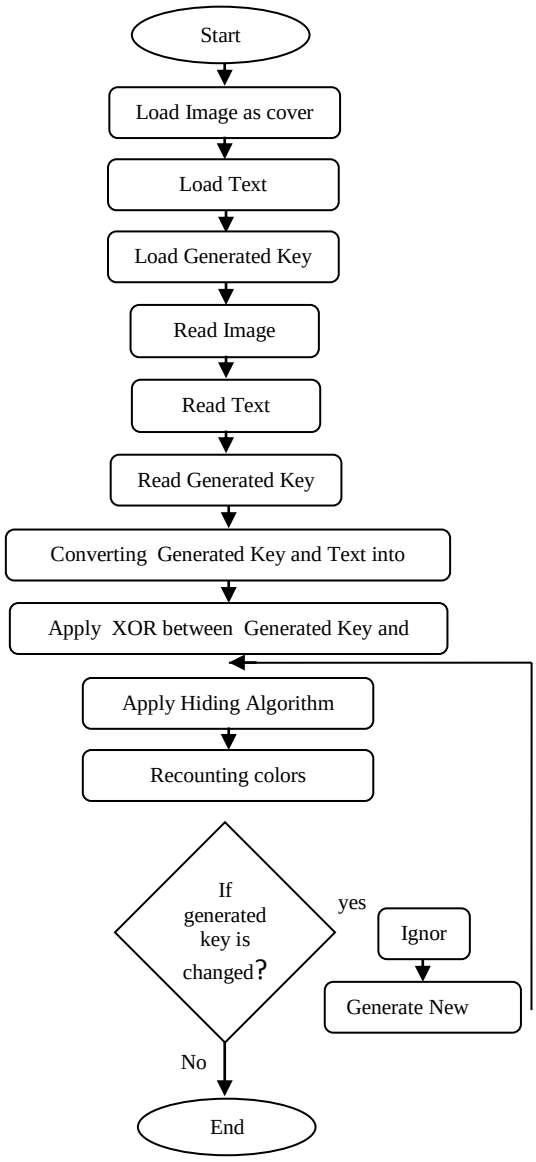

Figure 6: General flowchart of the testing via hiding

ii- Testing via Extension: the goal of this step is showing if color frequencies of an image are modified or not when the type of extension is transformed into another type of extension as shown in table (1). In this work, the original image has extension JPG. But in this step, the original image will transformed into five types of extensions. For each one of those extensions will notice what possible changes that can be happen, this step is shown in the figure (7) below:

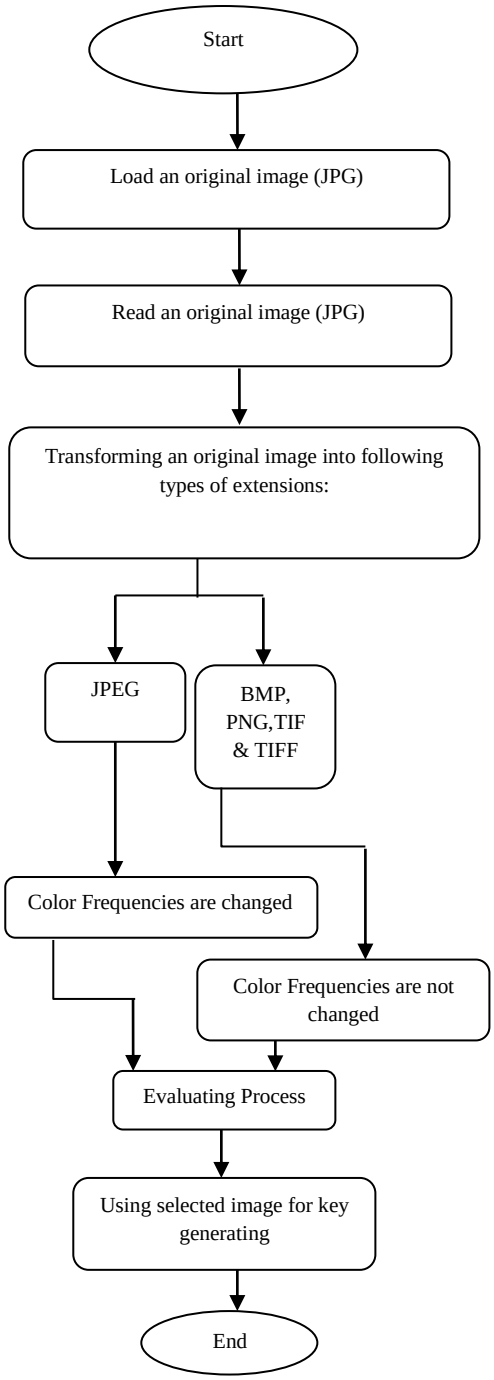

Figure 7: General flowchart of the testing via extension

Table 1: Testing via image extensions

Image Type	Color Image	Gray Image
BMP	Not Changed	Not Changed
PNG	Not Changed	Not Changed
TIF	Not Changed	Not Changed
TIFF	Not Changed	Not Changed
JPEG	Changed	Changed
JPG	Original Img.	Changed

IMPLEMENTATION PROCESS

When the proposed method for generating a private key from digital color image by using its feature is implemented, the general window of our is illustrated in Figure(8). Via implementation of proposed method practically, set of sub phases are mixed and performed in summarized manner in main menu. All basic and sub phases are divided into three main part as shown in Figure (8). The general window of proposed method is consist of three main parts that are: key generation (Key Gen.) part, hiding process part and showing process part. Each part of them will be explained with detail in the following.

Figure 8: General main window of proposed method

i. Key Generation Window: this window contains six parts that are image selecting, feature extraction, colors frequencies computing, maximum frequency computing, multiplication operation and addition operation parts. The first part is image selecting, which includes loading an image that used to extract required feature from it, The selected image is must be color. The required feature from loaded image will extracted via the second part of this window, the extracted feature is the colors of selected image such as red, green and blue.. After feature extraction, the colors frequencies will be computed via the third part of this window. The fourth part includes computing the maximum frequency for all colors of selected image. Finally, the multiplication and addition operations will performed to generate a cryptographic key via the fifth and sixth parts. The generated key is displayed in two forms, the first form is an integer and the second form is binary form. All parts of this window are illustrated in Figure (9). The preprocessing and converting processes are included in this part.

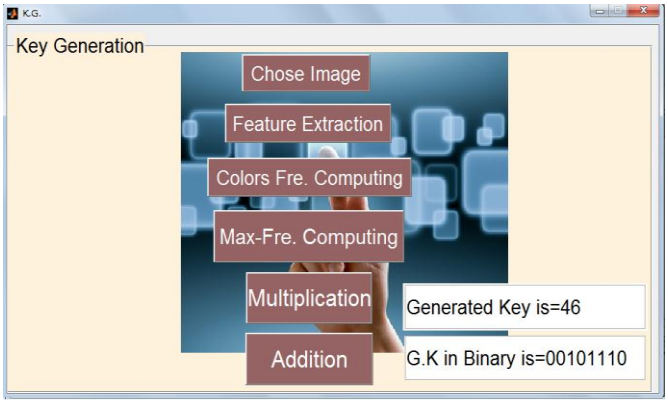

Figure 9: Key generation window

ii.Hiding Process Menu: this window consists of four parts that are cover image selecting, loading of generated key, text selecting and hiding operation. The main purpose of using hiding process in this proposed method is for testing a generated key by previous part, this process important for showing if a generated key is changed or not. Hiding process uses least significant bit (LSB) algorithm to hide secret information in positions of cover or host image that considered as least significant bit positions. The selected text that is as secret information must convert into binary form via this part. This window is illustrated in Figure (10).

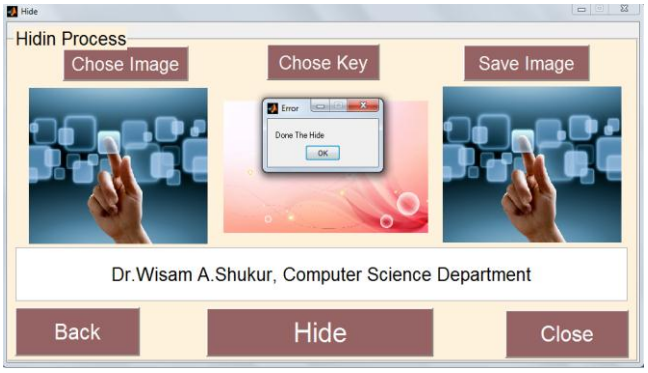

Figure 10: Hiding process window

iii.Showing Process Window: this window consists of two parts that are embedded image part and generated key part. The secret information that embedded in cover or host selected image by hiding process is extracted. After extraction process, the testing process is performed to show changing of a generated cryptographic key via recalculation color frequencies and determine range of differences between them before and after hiding process on cover image. The final result of testing process is no change on a generated cryptographic key by key generation process, this leads to fact

that a generated cryptographic key is robust. The encryption process that uses a generated cryptographic key by this proposed method is useful and good. Therefore, using this generated cryptographic key by the proposed method in cryptography system increases the security and complexity, then this made mission of attackers more difficult. This window is illustrated in Figure (11).

Figure 11: Showing process window

CONCLUSIONS

Using features of color image to generate a cryptographic key in cryptography system is new idea. This idea opens different orientations for scientific researchers to develop encryption methods to increase security and protection levels against unwanted or attackers attempts. From experiments of proposed method for different images, we can say that generating a cryptographic key from digital color image feature such as color is possible. By many experiments of proposed method and its results, there are many points that concluded in this work as shown in the following:

1) The generated cryptographic key is not changed or modified although hiding a text in an image.
2) Improving the hiding and testing processes via hiding an image in an image instead hiding a text in an image.
3) Using another feature of digital color image to generate a cryptographic key instead color .
4) Using more than image to generate a cryptographic key.
5) To increase complexity of a generated cryptographic key, applying extra operation such XOR or others on the result generated cryptographic key.
6) Adding different types of noises to cover image after hiding process such as Gaussian , poison , speckle and salt& pepper to check if generated cryptographic key is changed or not?
7) Using watermark technique for testing a generated cryptographic key by involving watermark in cover image then assessment quality of it to show contrast between original and extracted watermarks by using NC, PSNR and MSE as quality metrics.

REFRENCES

[1] Eric Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", 2003.

[2] William S. **"**Cryptography and Network Security Principles and Practices**"**, 2011.

[3] David Groth, "Network, Study Guide ", third Edition, Sybex, Inc., Alameda,CA,2002.

[4] Glover, P. and M. Grant," Digital communications",2nd Edition, Person Education,2004.

[5] Wenbo M. , "Modern Cryptography: Theory and Practice**"**, Prentice Hall, ISBN: 978-0132887410, 2006.

[6] Chey Cobb, "Cryptography for Dummies", 2004.

[7] William S., **"**Cryptography and Network Security Principles and Practices**"**, Prentice Hall, Fourth Edition, ISBN: 978-0131873162, 2005.

[8] William S., "Network Security Essentials: Application and Standards", Pearson Education, ISBN: 978027379336, 2011.

[9] Charles P. P. and Shari L. P., "Security in Computing, Fourth Edition", Prentice Hall, Fourth Edition, ISBN: 978-0132390774, 2006.

[10] David G., "Network+ ™, Study Guide, 3rd Edition, SYBEX, 2002.

[11] Glover, P. and Grant M., "Digital Communications", 2nd edition, 2004.

[12] Ziyad Tariq Mustafa Al-Ta'i, "Development of Multilayer New Covert Audio Cryptographic Model ", International Journal of Machine Learning and Computing, Vol. 1, No. 2, June 2011.

[13] F. N. Johnson, D. Zoran and J. Sushil "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures", Kluwer Academic Publishers, Advances in Information Security, 2001.

[14] Fridrich J., Goljan M., Hogea D. and Soukal D., " Quantitative steganalysis of digital images: estimating the secret message length, *Multimedia Systems* **9**(3), 288–302, 2003.

[15] Cox I., Miller M., Bloom J., Friedrich J. and Kalker T., "Digital Watermarking and Steganography", 2nd ed., Morgan Kaufmann, 2007.