IMAGE STEGANOGRAPHY BASED INFORMATION SECURITY SYSTEM

[1]ZIN MAY ZAW, [2]SU WAI PHYO

[1,2]Department Of Information Technology, Mandalay Technological University The Republic Of The Union Of Myanmar
E-mail: [1]zinmay83@gmail.com, [2]suwaiphyo@gmail.com

Abstract- In today's data communication environments, information security is an important issue in data storage and transmission. Due to the security attacks that made on data communication, effective data hiding systems are needed to develop for information security. Steganography and cryptography are both ways to protect information security and concealing it. Thus, to solve the serious problem of security requirements, this work proposes information security system by using the integration of cryptography and image steganography. The purpose of this system is to enhance the security of hidden message by improving the security of cover image. To create the encrypted cover image, the combination of image transformation and encryption technique is effectively used. Firstly, the original image is transformed with optimized block-based transformation algorithm to obtain better robustness of image encryption. And then, the transformed image is encrypted by using Blowfish encryption algorithm. After getting the encrypted image, the secret message is hidden within this image which is used as a cover by using LSB embedding technique for information security. Moreover, to prove the advantages of combination process (optimized transformation and Blowfish encryption), performance comparison is made by calculating the correlation and entropy of encrypted images generated by combination process and single Blowfish encryption.

Index Terms- Cryptography, Steganography, Transformation, Blowfish, Correlation, Entropy.

I. INTRODUCTION

The wide spread use of internet for communication has increased the attacks to users. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. Steganography is the best way of hiding secret message in innocuous media (carriers) such as text, image, audio, video and protocol. Among these different carriers, digital image is the most popular cover object because large amount of redundant bits are presented in the digital representation of an image [1]. Therefore, this work proposes secure information hiding system in encrypted cover image by using the combination of steganography and cryptography. Because of using encrypted cover image, the attacker cannot know that whether or not secret message is present within encrypted image and they will notice to attack only the content of encrypted cover image. Thus, it can get high security for hidden message.

There are many data hiding techniques for image steganography. Among them, Least Significant Bit (LSB) insertion is very popular and simple technique for embedding information into cover image [2]. On the other hand, this paper intends to enhance the security of hidden message by improving the security of encrypted cover image. Not only Blowfish encryption algorithm but also transformation algorithm is effectively used to enhance the security of cover image. But, according to many research areas, neither of transformation and encryption technologies alone is secure against various attacks [3]. For this reason, a block-based image transformation algorithm is optimized to combine with Blowfish algorithm in this information hiding system. Moreover, performance comparison is made by calculating the correlation and entropy value of encrypted images, to know the usage of extra transformation process in image encryption.

II. LITERATURE REVIEW

With the rapid growth of internet usage in today's communication system, data security has become a fundamental issue. Therefore, new proposed algorithms to enhance the security requirements are developed in order to get efficient reliability in many research areas. In [4], Dr. Fadhil Salman Abed proposed encoding and hiding text in an image by using the combination of RSA crypto system and image steganography approach for security and more robust manner. In his work, a new hiding method is proposed based on encoding the information by using RSA cryptosystem and hiding the cipher information (ciphertext) by using his proposed fractal image compression (FIC). Then, Min Wu and Bede Liu [5] also proposed a new method to embed data in binary images, including scanned text, figures, and signatures. The method manipulates "flippable" pixels to enforce specific block based relationship in order to embed a significant amount of data without causing noticeable artifacts. They have applied shuffling before embedding to equalize the uneven embedding capacity from region to region. The hidden data can then be extracted without using the original image, and can also be accurately extracted after high quality printing and scanning with the help of a few registration marks.

Moreover, Dr. S.Kishore Reddy [6] also proposed encrypted data hiding system in encrypted cover

images. In his experiment, the author used three encryption methods such as RSA, reversible data hiding method and cat map transform to encrypt the image and then secret information is embedded within the encrypted image by using LSB embedding technique. Moreover, the performance comparison was made between these three methods in term of Peak Signal to Noise Ratio (PSNR) values. The author intended to enhance both image and data security by studying the various encryption schemes.
According to the literature and concepts of security enhancement approaches which are pointed out from the previous researches, the main aim of this work is to propose information security system based on image steganography and cryptographic algorithm.

III. BACKGROUND THEORY

For the information security, LSB embedding technique is used to hide secret message within encrypted cover image. Moreover, the two main theories used for image security are Blowfish encryption and optimized block-based transformation algorithm. Then, correlation and entropy are also calculated to know the advantage of using extra transformation process for image encryption rather than single encryption.

A. Least Significant Bit (LSB) Insertion

Information can be hidden many different ways in images. One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. It is a simple approach in which the least significant bits of the cover-image are altered so that they form the embedded information.

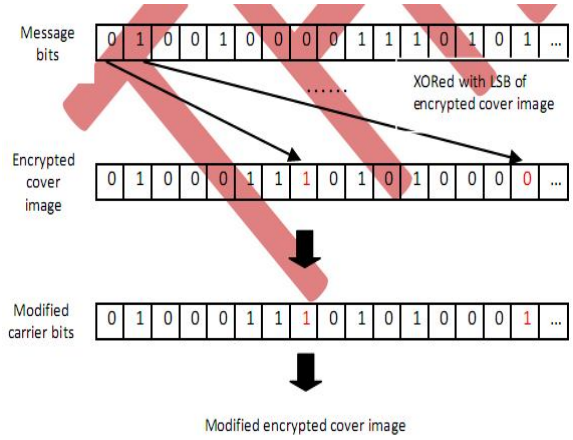


Fig. 1: Inserting the message bits into LSB of the cover image [7]

Fig.1 shows the example of hiding the secret message into encrypted cover image by using LSB embedding technique. Firstly, the image data and secret message are accessed as a series of bits [8]. Then, the bits of the secret message are inserted into the LSB of the bytes of the encrypted cover image by using XOR operation. On average, only half the bits in an image will need to be modified to hide a secret message using the maximum cover size [9].

B. Optimization of Block-based Transformation Algorithm

In order to enhance image security, a block-based image transformation algorithm is optimized to combine with Blowfish encryption in this work. The algorithm is as follows:

(1) Load image
(2) Input key
(3) Get image width and high
(4) Divide image into n x n pixel blocks
(5) Calculate horizontal pixel blocks = Int (Image width/n)
Calculate vertical pixel blocks = Int (Image high/n)
(6) Calculate the number of pixel blocks = Horizontal pixel blocks x Vertical pixel blocks
(7) Seed = Hash value (key)
(8) Randomize ()
(9) I = 0, Count=0
While I < Number of pixel blocks
R= random number between 0 and number of blocks -1
While R is selected block number and Count < 500
R = random number between 0 and number of blocks -1
If R is selected block number then
Count = Count+1
Else
Count = 0
End if End while
I - R
I + = 1
End while

C. Blowfish Encryption Algorithm

Blowfish is a symmetric encryption algorithm, which makes the use of the same secret key for both encryption and decryption of the message. It is a block cipher which means that it divides the message into blocks of fixed length during encryption or decryption. Block diagram of Blowfish encryption process is shown in Fig. 2.

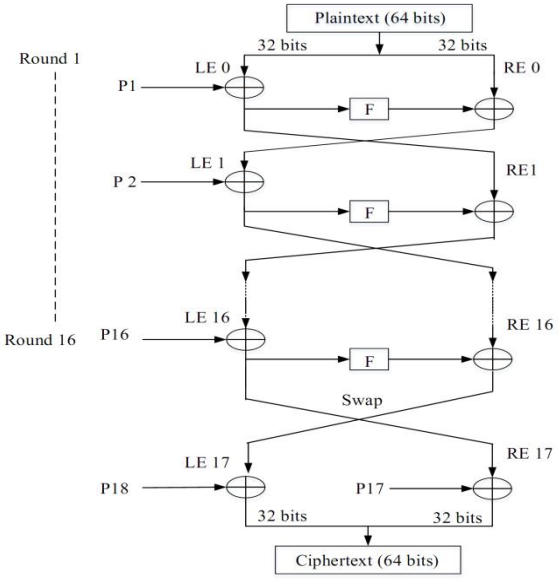


Fig. 2: Block diagram of Blowfish encryption

Blowfish encrypts 64-bit block of plaintext as input and produces corresponding 64-bit block of ciphertext as output. It takes variable length key, ranging from 32 bits to 448 bits. Its structure is based on 16 round Feistel network [10]. This algorithm is used as an alternative for DES (Data Encryption Standard) or IDEA (International Data Encryption Algorithm). The algorithm consists of two parts: key expansion part and data encryption part. Key expansion part: It converts a key of at most 448 bits into several sub key arrays, totaling 4168 bytes. Data encryption part: In data encryption part, 16-round Feistel network is used. Each round consists of a key dependent permutation and a key and data dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. Decryption process is similar to encryption except that in decryption, the P-entries, P1, P2,…, P18 are used in reverse order.

D. Entropy and Correlation

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [11]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy H(m) of a message source can be measured by equation (1).

$$H(m) = -\sum_{i=0}^{m-1} p(m_i) log_2 p(m_i) \quad (1)$$

where m is the total number of symbols, mi □ m and p(mi) represents the probability of occurrence of each symbol mi. Logarithm of base 2 denotes that the entropy is expressed in bits.

Correlation is a statistical measure of image security that expresses a degree of relationship between two adjacent pixels in an image. In most of the natural images, the values of neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). The aim of correlation measure is to keep the amount of redundant information available in the encrypted image as low as possible [12]. It is calculated by using equation (2).

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{(n\sum(x^2) - (\sum x)^2)(n\sum(y^2) - (\sum y)^2)}} \quad (2)$$

where

r = correlation value

n = number of pairs of adjacent pixels randomly selected from an image

x and y = the intensity values of two neighboring pixels in image

IV. SYSTEM ARCHITECTURE

The general process of system design is shown in Fig. 3. This information hiding system is mainly composed of two portions: creating encrypted cover and embedding information within this cover.

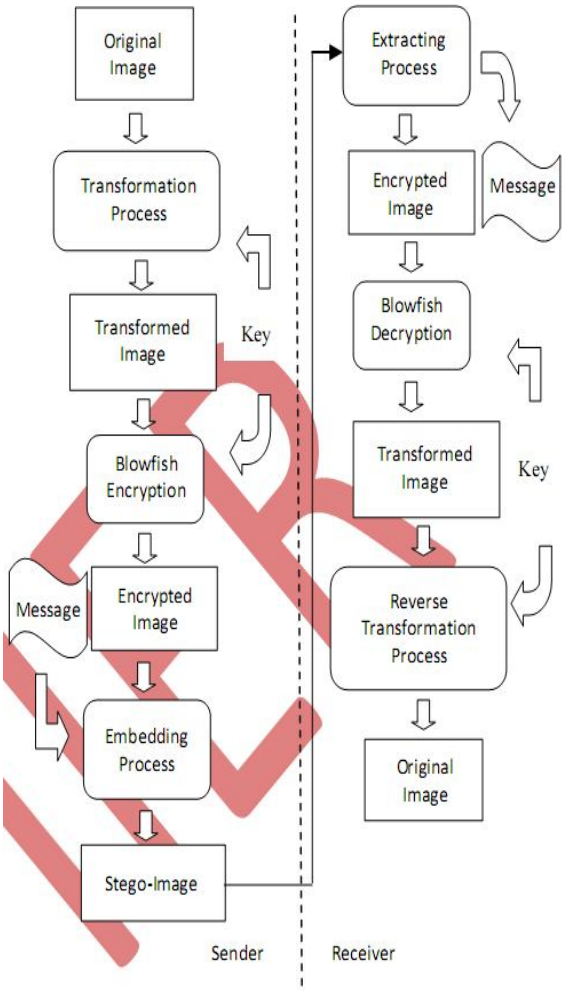


Fig. 3: General block diagram of image steganography based information security system

In the process of creating encrypted cover image, the original image is firstly transformed with optimized block-based transformation algorithm to obtain better robustness of image encryption. And then, the generated transformed image is encrypted by using Blowfish algorithm with secret key. After getting the encrypted image, the secret message is hidden within it as a cover object by using LSB embedding technique and stego-image is generated. Finally, the stego-image is transmitted to the receiver site through the insecure channel. At the receiver site, the hidden message is firstly extracted by using extracting process and the original image can be retrieved by using image decryption and reverse transformation process.

V. SYSTEM IMPLEMENTATION

This information security system using encrypted cover image is implemented by using C# programming language. Implementation results are presented as a series of interfaces. The main interface is illustrated in Fig. 4. There are two buttons to select for image encryption: “Blowfish Encryption” and “Proposed Combination Process” buttons.

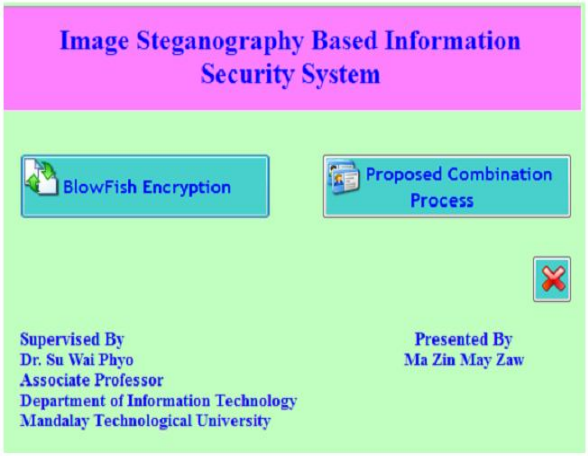


Fig. 4: Main Form

If the user selects "Blowfish Encryption" button, the original image is encrypted with Blowfish by using "Encrypt" button. After getting the encrypted image, the secret message is loaded by using "Read Text File" button and hides it within encrypted image using "Hide" button. Then, the generated stego-image is saved by using "Save Stego-Image" button as shown in Fig. 5.

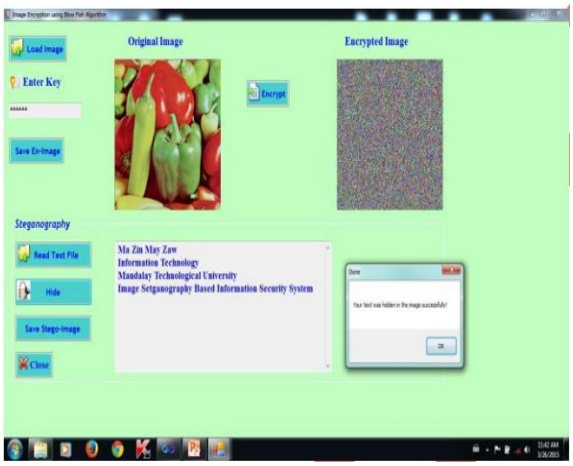


Fig. 5: Single Blowfish Encryption and Data Hiding

At the receiver site, the data extraction and decryption processes must be performed as shown in Fig. 6.

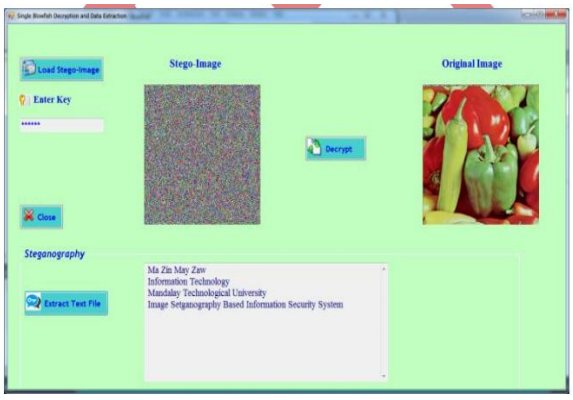


Fig. 6: Data Extracting and Single Blowfish Decryption

On the other hand, if the "Proposed Combination Process" button is selected in the main interface, the original image is firstly needed to transform by using optimized block-based image transformation algorithm as illustrated in Fig. 7. In the transformation process, the original image is loaded and the key is inserted. Key is the main role in creating transformation table.



Fig. 7: Transformation Process

After getting the transformed image, it is encrypted by using Blowfish algorithm as shown in Fig. 8. Then, the secret message is hidden within encrypted image by using "Hide" button to obtain the stego-image.

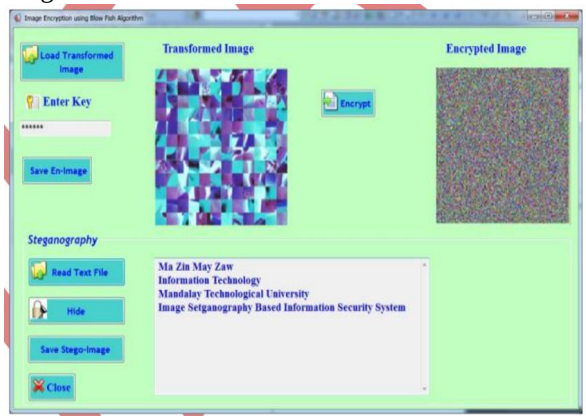


Fig. 8: Combination Process and Data Hiding

At the receiver site, the stego-image is reloaded and then extracts the secret information.

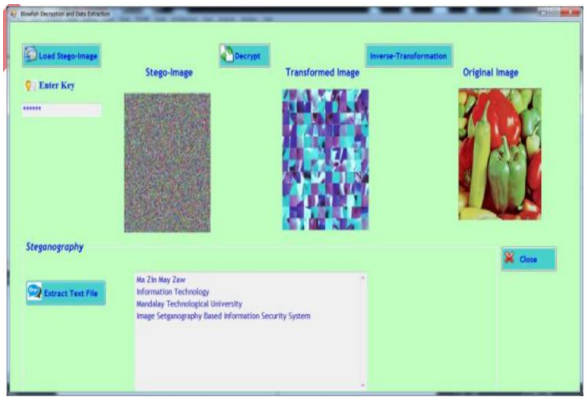


Fig. 9: Data Extracting and Combination Process

Next, the original image can be retrieved by using the "Decrypt" and "Inverse-Transformation" buttons as illustrated in Fig. 9.

VI. PERFORMANCE EVALUATION

This section shows the robustness of using combination process (optimized block-based transformation algorithm and Blowfish) for image security by calculating correlation and entropy value. These values are calculated on encrypted images generated by not only combination process but also single Blowfish algorithm in order to show the comparison results. The selected original bmp image which is the size of 256 x 256 pixels with 256 colors, and its encrypted images are shown in Fig. 10.

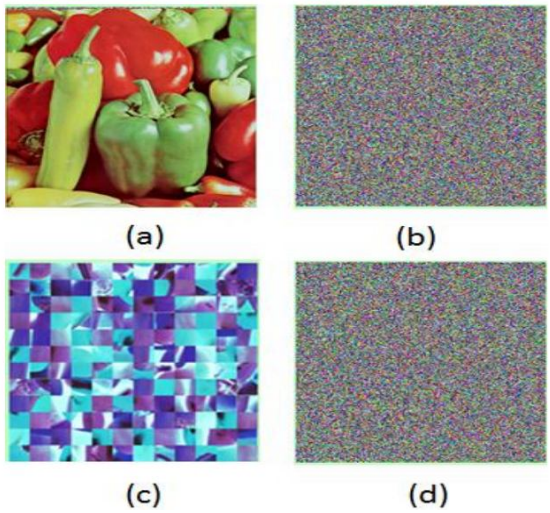
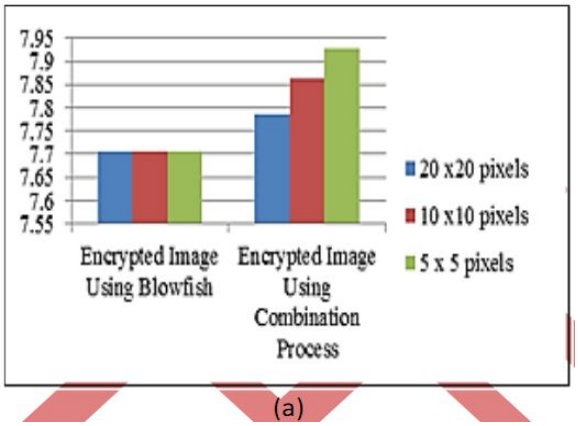


Fig. 10: (a) original image (b) encrypted image using Blowfish (c) encrypted image using transformation algorithm (d) encrypted image using combination of transformation and Blowfish encryption

To evaluate the impact of the number of block size on correlation and entropy value, the image is tested by dividing three different number of block sizes such as 20x20 pixel blocks, 10x10 pixel blocks and 5x5 pixel blocks in this system. The analytical results of entropy and correlation are shown in Fig. 11 (a) and (b) respectively.



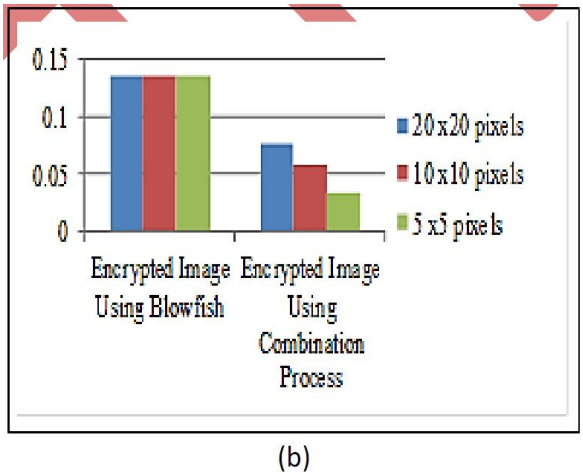


Fig. 11: Experimental results on three different block sizes (a) entropy (b) correlation

According to the analytical results, the combination process has lower correlation and higher entropy value rather than single blowfish algorithm for all three different tests. Moreover, it can be seen that the smaller the block sizes, the higher the security.

CONCLUSION

This system focuses on information hiding system by using encrypted cover image. Due to the usage of encrypted cover image, the attacker can't easily suspicious that the secret information is hidden in it and they will only try to decipher the encrypted cover image. Moreover, this system is also intended to enhance the security of hidden message by improving the security of encrypted cover image. According to the comparison results, there is lower correlation and higher entropy value when the optimized transformation algorithm is applied as pre-encryption step. Therefore, it can give better image security, rather than the usage of single Blowfish. By using the LSB embedding technique for information security, it can also provide the security requirements such as confidentiality of hidden message. For embedding and extracting processes, LSB is very simple technique. As further extension, it can be optimized to obtain the better embedding capacity without degradation the cover image quality. In this system, only two image types such as bmp and jpg can be used as the cover images. This information hiding system can be applied in many security awareness application areas such as military and medical imaging system.

REFERENCES

[1] Morkel, T., Eloff, J. H. P., and Olivier, M. S.: "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, South Africa, 2002.

[2] Moulin P and Koetter R, "Data-Hiding Codes", Proceedings of the IEEE, pp. 2083-2126, 2005.

[3] Li. Shujun, Li. Chengqing and C. Guanrong, "A general cryptanalysis of permutation-only multimedia encryption algorithms", Fellow, IEEE. Available: http://eprint.iacr.org / 2004.
[4] Dr. Fadhil Salman Abed, "A proposed encoding and hiding text in an image by using Fractal Image Compression", International Journal on Computer Science and Engineering (IJCSE), vol. 4, no. 01, January, 2012.
[5] Min Wu and Bede Liu, "Data hiding in binary image for authentication and annotation", IEEE Tanss, Image Processing, vol.6, Issue 4, pp. 528-538, August 2004.
[6] Dr. S. Kishore Reddy, "Encrypted data hiding in encrypted images", International Journal of Research in Engineering and Applied Sciences, vol.2, pp. 50-59, September 2012. Available: http://www.euroasiapub.org.
[7] Nilar Shein Lwin: "New Embedding Method Based on Stego-key Length", The 4th International Conference on Science and Engineering (ICSE), Yangon, Myanmar, December, 2013.
[8] Andrew Davison: "Java Prog. Techniques for Games. Java Art", Ch. 6, Draft #1, June 2009.
[9] Krenn. R.,"Steganography and Steganalysis", http://www. krenn.nl/ univ/cry/steg/article.pdf.
[10] B. Schneier, Applied Cryptography, John Wiley and Sons, New York, 1994.
[11] Shannon C.E, "Communication theory of secrecy systems", Bell System Technical Journal, pp. 656-715, 1949.
[12] Burger W. and M. Burge, Digital Image Processing: An Algorithmic Introduction Using Java, Springer-Verlag, New York, 2008.

★★★