Int. j. inf. tecnol. (June 2019) 11(2):373–379
https://doi.org/10.1007/s41870-018-0259-0

ORIGINAL RESEARCH

Histogram and entropy based digital image watermarking scheme

Sunesh Malik[1,2] · **Rama Kishore Reddlapalli**[1]

Received: 16 January 2018 / Accepted: 14 November 2018 / Published online: 24 November 2018

Abstract In today's era, Fortifying robustness and imperceptibility of digital watermarking has become non trivial. In this paper, a digital image watermarking algorithm based on entropy of blocks and histogram is proposed to improve imperceptibility. In this, first host image is divided into blocks and then blocks are culled on the basis of entropy value for watermark embedding. After that, watermark is embedded into selected blocks by using histogram shape method. Histogram shape method divides selected blocks into groups and further locations of pixels within groups are identified for watermark embedding. Histogram shape method makes algorithm more robust against attacks. The integration of block based histogram shape approach and entropy makes algorithm more imperceptible. Experiment results demonstrate that proposed method has an excellent imperceptibility. Proposed method also resists against noise and scaling attacks.

Keywords Digital image watermarking · Entropy · Histogram · Imperceptibility · Watermark

✉ Sunesh Malik
suneshmlk@gmail.com

Rama Kishore Reddlapalli
ram_kish@yahoo.com

[1] University School of Information and Communication Technology, GGSIPU, Dwarka, India

[2] MSIT, Janakpuri, New Delhi, India

1 Introduction

In today's world, the furtherance of technology has made transmission and computing of digital images fast and efficient. But on the flipside, it originates several issues like unauthorized duplication and manipulation etc. Unauthorized duplication and manipulation cause security concerns over digital images. To deal with the above mentioned issues, digital watermarking comes into light as a key solution. Digital watermarking is a technique which injects watermark into digital image to deal with the distinct security issues [1, 2]. Watermark is in the form of bit pattern or author information [3]. Watermark may be text, image, logo etc. Watermark information can be injected into the spatial domain or frequency domain of the host image [4, 5].

Before inserting watermark, host image is processed into one of the above mentioned domain. In spatial domain, image is represented in form of pixels and embedding of the watermark is performed by modifying pixel values. Whereas transform domain expresses image in the form of frequencies. Different transforms are used in digital watermarking like DCT, SVD, DWT, and DFT etc. to represent image in frequency domain [6, 7]. In transform domain based digital image watermarking techniques, image is first converted into predefined transform and then watermark embedding is performed.

Each and every domain has its own intrinsic attributes and embedding method. So, digital watermarking techniques are inferred by its traits. The main traits of watermarking are imperceptibility and robustness. Robustness is the competence of extracting concrete watermark after sustaining attacks and imperceptibility implies that watermark should not be perceptible [8].

A lot of watermarking methods have been acquainted in the history on above traits. Few of them are robust but do not cope up well with imperceptibility. To work with above mentioned trait, Concept of entropy is exploited in this work. Entropy is a statistical measure used for characterizing texture of image. Entropy computes the randomness of image and randomness characterizes the texture content of image. Texture plays a vital role in human visual perception [9]. By keeping this frame of reference, entropy has been contemplated for improving perceptual quality of image.

In this paper, entropy is fused with histogram shape method. For maintaining robustness, histogram shape trait is considered [10–12]. The aid of entropy and histogram shape method together helps in enhancing imperceptibility and also maintaining robustness.

Histogram for eight bit gray scale image can be defined by Eq. 1 in which, ht(i) represents number of pixels whose pixel value is i and i denotes gray level of image. Eight bit gray scale image carries 256 gray levels lies from 0 to 255.

$$\mathrm{Ht(i)} = \{\ \mathrm{ht(i)} | \mathrm{i} = 0, 1, \ldots\ldots, 255\} \quad (1)$$

Histogram is statistical concept used to imply pixel distribution of digital image but it is unable to trot out about spatial relationship of pixels [11, 13–15]. Property of image histogram helps in acquiring resistance against geometric attacks [10–12]. A lot of image watermarking techniques in literature have utilized the concept of histogram for embedding and extracting of watermark. Work related to entropy and histogram will be presented in Sect. 2.

The rest of this paper is framed as follows. Section 2 provides a brief reviews on entropy, block and histogram shape based methods. Section 3 illustrates about proposed embedding process and Sect. 4 states proposed extraction process. Experimental results are discussed into Sect. 5. Section 6 illustrates conclusion and future scope.

2 Background review

This section reviews the work reported in history related to entropy and histogram shape approach. Mainly, watermarking techniques use concept of histogram for inserting watermark into host image and concept of entropy for analyzing image.

Deng et al. [16] reported local histogram based image watermarking method by integrating local circular regions with histogram to achieve robustness against geometric and common signal processing attacks. Initially, features of image are extracted by utilizing Harris Laplace detector and then local circular regions are formed. Non overlapped local circular regions are selected for watermark embedding. Watermark is embedded by modifying the shape of local histogram.

Lusson et al. [17] presented a hybrid digital watermarking technique which exploits the RGB and YCbCr color spaces by utilizing spatial domain techniques to gain robustness and to hide watermark in such a way that it becomes undetectable. In this watermarking method, embedding process is divided into two phases. In the first phase, host image is decomposed into three channels called red, green and blue in RGB color space and then watermark is inserted into all three color channels. In second phase, combined RGB image is converted into Y, Cb, Cr channels of YCbCr color space. Here, only two channels Cb and Cr are used for embedding watermark. This color space put limits on size of watermark to be inserted. This watermarking method is robust, invisible, secure and complex.

Xiang et al. [18] proposed a histogram based image hashing method in order to gain robustness to geometric deformations. In this method, image is pre-processed by means of Gaussian filtering to improve hash robustness. Hash function utilized in this method is simple to implement. Robustness of image hashing method is achieved by employing property of histogram shape invariance. This method has satisfactory results against geometric and common signal processing attacks.

Singh et al. [19] reported image watermarking method based on entropy to improve imperceptibility and robustness. This method embeds two watermarks i.e., one is low frequency watermark and other high frequency watermark. Watermark is inserted in high entropy value area of host image. Further DWT and SVD are applied for embedding watermark.

Xuefeng et al. [20] presented a histogram shape watermarking algorithm which attains robustness against geometric and image processing attacks. In this, histogram modification scheme is employed with use of mean square error for block selection to be modified.

Wang et al. [14] classify histogram based approach into two sections. First, modifies histogram vector to specified one whereas second section maintains histogram original features. The authors also proposed a watermarking algorithm based on histogram shape in order to resist geometric attacks. In this, original image histogram is modified based on statistical characteristics and binary watermark.

Zong et al. [11] presented a histogram shape method in order to attain resistance against cropping and random bending attacks etc. In this, watermark is inserted by means of bin shifting within group by maintaining histogram shape.

Zong et al. [12] reported a histogram shape method in which histogram frequency component modification is employed in order to improve robustness against cropping

and random bending attacks. HFCM also reduces the side effects of Gaussian filtering. Kiran et al. [10] also proposed histogram based approach in which watermark is inserted by maintaining histogram shape. In this watermarking algorithm, Butterworth filter is employed instead of Gaussian filter.

Xuansen et al. [13] reported watermarking algorithm based on histogram modification that is resistant to geometric attack. Watermark is embedded by bin modification. In this, only one bin is modified out of adjacent bins. This is not robust against key estimation attack.

Chrysochos et al. [21] presented a hybrid watermarking method which inserts two watermarks and attains robustness robust against filtering, noise and compression attacks. First watermark is inserted by employing chaotic function and correlation method. Second watermark is embedded in luminosity of histogram by means of histogram modification.

Chen et al. [22] presented audio watermarking technique by utilizing concept of wavelet based entropy and achieve robustness against the attacks like resampling, MP3 compression, low pass filtering and amplitude scaling. In this, low frequency coefficients of DWT are transformed into wavelet based entropy domain. Then watermark is embedded. Watermarked is extracted only by values of wavelet based entropy.

Yang et al. [23] reported an information masking model in spatial, spectrum and temporal domain in order to improve the performance in terms of imperceptibility and robustness. Concept of entropy is exploited in this method to improve imperceptibility and robustness.

Kumar et al. [24] presented digital image watermarking technique by block entropy. LSB substitution method is employed for watermark embedding. In this paper, block with high entropy value are utilized for watermark embedding.

On the basis of above mentioned papers, a block entropy based watermarking method is proposed for gray scale image. The proposed method embeds watermark in selected blocks of gray scale image instead of full host image. Blocks are picked on the basis of entropy value. Watermark is embedded in the selected blocks by using histogram shape method. Afterwards, within blocks gray levels are divided into groups. Within blocks, few blocks are excerpted for watermark embedding and an embedding rule is established that embeds watermark information. One group carry only one watermark bit information. As watermark embedding process is reversible, watermark bit is extracted by finding relationship between pixel values of bins in the group.

3 Proposed embedding process

Proposed watermarking method has been designed for improving imperceptibility. Entropy and histogram shape method is employed in proposed embedding and extraction process. Watermark embedding contains two phases. First phase is called pre-processing and other is watermark embedding. To embed watermark, Image histogram construction is required. Eight bit gray scale image is utilized. Gray histogram is straightforward but an important statistical expression. Image histogram symbolizes number of pixels versus the gray scale values. If the original image is not gray scale then its color space is converted into gray scale.

3.1 Preprocessing

In pre-processing, host image is processed by converting image to blocks and entropy is calculated for every block. Initially, read the input host image. If host image is not in gray-scale then it is converted into gray scale. Gray scale image is partitioned into 16×16 equal size blocks. Entropy is calculated for each block as follows [19, 25].

$$E = -\sum_{i} P_i \log_2(P_i). \tag{2}$$

Entropy acquires the highest value when all elements in P matrix are equal [9] Image areas with high entropy value are least visible to human. If watermark is inserted in high entropy area then higher imperceptibility can be achieved. Therefore, Blocks having high entropy value are selected for watermark embedding.

3.2 Watermark embedding procedure

As mentioned in previous section, high entropy blocks are selected for watermark embedding. Watermark embedding is done by using histogram shape property [10, 11]. This method uses 256 level gray scale image histogram ranging from 0 to 255. Watermark embedding is done to each block using the following steps.

Step1. Histogram Construction: generate histogram for each selected block of host image.

$$HS(i) = hs(i) | i = 0, 1, \ldots\ldots, 255 \tag{3}$$

Where hs (i) denotes number of pixels of intensity value i.

Step 2. Embedding Location selection within Block: in this step, further embedding location is culled within block. For this, two gray levels are combined as a bin and two neighboring bins as a group in manner of given Eqs. 4 and 5, respectively:

$$Bn(i) = hs(2 \times i) + hs(2 \times i + 1), \quad (4)$$

$$Gp(i) = Bn(2 \times i) + Bn(2 \times i + 1). \quad (5)$$

Number of pixels in ith group is N_g. Selection of embedding location within block depends on N_g and threshold denoted as T_2. Threshold T_2 is calculated based on following formula:

$$T_2 = \alpha \times M \times N, \quad (6)$$

whereas M denotes number of rows and N denotes number of columns. Value of α is taken as 0.008. Groups having value greater than threshold T_2 is selected for watermark embedding.

Step 3. Watermark Embedding: each Selected group will be used for holding watermark bit. Random binary bit sequence is used as a watermark. Watermark is embedded in selected groups of culled block. Watermark bit sequence is represented as.

$$W = \{ w(k) | k = 0, 1, \ldots\ldots\ldots\ldots\ldots L \} \quad (7)$$

Length of watermark sequence is denoted by L. The embedding rule for watermark bits is as follows:

$$\text{If } W(k) = 1 \text{then } \frac{NBn1}{NBn2} \geq T_3, \quad (8)$$

$$\text{If } W(k) = 0 \text{then } \frac{NBn2}{NBn1} \geq T_3, \quad (9)$$

where W is watermark bit and NBn1 denotes number of pixels in bin 1 and NBn2 represent number of pixels in bin2.

Pixels for holding watermark bit are randomly chosen in Bn1 and Shifted into Bn2 in case of embedding watermark bit 0 and vice versa in case of watermark bit 1. Randomly chosen pixel is notated by $P0_{RC}$ and $P1_{RC}$. $P0_{RC}$ and $P1_{RC}$ are fetched as follows:

$$P0_{RC} = \frac{2 \times NBn1 - NBn2}{3} \text{ and } P1_{RC} = \frac{2 \times NBn2 - NBn1}{3}. \quad (10)$$

This process is repeated until all watermark bits are embedded.

Step4.Watermarked image: after performing watermark embedding, processed and unprocessed blocks of gray scale image is combined. At last, watermarked Image is produced finally.

4 Proposed extraction process

The process of watermark embedding is invertible. This makes watermark extraction simple. Extraction process receives watermarked image as an input. Watermark decoding processing follows the similar steps as in the embedding process. Main aim at decoding is to acquire the estimate of watermark sequence.

In extraction process, first watermarked image is divided into 16 × 16 equal size blocks and entropy is calculated for each block. Afterwards, Blocks having high entropy value are selected for watermark extraction in same manner as in embedding phase.

Gray scale histogram is calculated for each selected watermarked block and form groups in histogram by combining histogram bins. Each group contains two adjacent bins named as Bn1 and Bn2. Then hold the watermarked groups with most number of pixels based on calculated threshold T_1. Watermark bits will be extracted by adopting following rule.

1. First, calculate number of bits in Bn1 and Bn2, respectively in every selected watermarked group. Then computing ratio between Bn1 and Bn2 as given below:

   $$\text{Ratio} = \frac{Bn1}{Bn2}.$$

2. By computing ratio, one embedded bit is extracted in reference to following expression:

   if Ratio $\geq$ 1then,

   W'(k) = 1,

   Else,

   W'(k) = 0,

where W' denotes extracted watermark sequence. Extracted watermark sequence is depicted as:

$$W' = \{ w'^{(k)} | k = 0, 1, \ldots\ldots\ldots\ldots\ldots L \}$$

This process is repeated until all bits are extracted.

5 Experimental results

Performance of proposed watermarking method is measured by means of perceptual quality and robustness. In this experiment, three well known gray scale images named Barbara, Lena, and Pirate (size 256 by 256) are used as host images [26, 27]. A 45 bits PN sequence is used as watermark information. In order to measure imperceptibility and robustness, two quality parameters i.e., peak signal to noise ratio (PSNR), bit error rate (BER) are used. Quality parameter BER corresponds to extracted watermark. BER is computed between original watermark and extracted watermark. BER computes the number of differing pixels between original watermark and extracted watermark.

Watermark imperceptibility is an estimate of distortion amount in the host image due to watermark embedding. In this, distortion amount is related to block entropy threshold and thresholds used in embedding procedure. In this method, threshold is related to perceptual quality and length of watermark. Greater the value of threshold of block entropy threshold then imperceptibility will be higher. Watermark imperceptibility is measured by PSNR value [13]. PSNR above 40DB indicates good perceptual quality [11].

The quality parameter PSNR is used to measure perceptual quality and corresponds to watermarked image. The original and corresponding watermarked images are shown in Fig. 1. Table 1 validates the proposed method has high PSNR corresponding to watermarked image. PSNR is measured in terms of DB.

Hence, the Experimental results demonstrate that watermark imperceptibility of our proposed algorithm is excellent. Results of host and watermarked image are shown in Perceptual quality Table 1.

Table 1 PSNR Values of the proposed method

PSNR	Lena	Barbara	Pirate
	74.3644	67.7891	62.4682

The histograms of original and watermarked images are shown in Fig. 2. When histograms of original images are compared with watermarked histogram, it is found that watermarked images maintain original image information. The difference between original and watermarked histogram is observed in form of interstices because embedding introduces changes only in adjacent bin.

The robustness of proposed method is checked by applying different attacks on watermarked image and then extracted the watermark. Robustness of proposed scheme is measured in terms of bit error rate called BER. Tables 2, 3 exhibits results of watermark extraction after addition of attacks. The attacks applied on three images are rotation,

Fig. 1 Watermarked images corresponding to original images [26, 27]

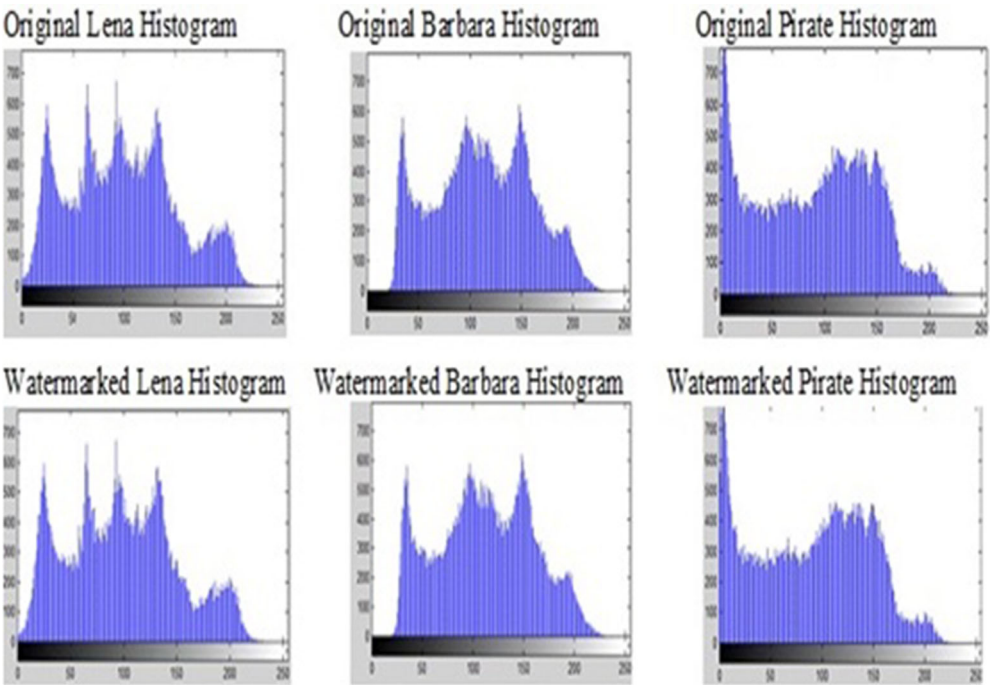

Fig. 2 The histograms of original and watermarked images

Table 2 Bit error rate (BER) of proposed watermarking scheme

Attacks	Lena	Barbara	Pirate
Rotation	0.1500	0.3864	0.0714
Noise	0.0851	0.0909	0.0233
Cropping	0.2553	0.2093	0.3488
Scaling	0.1957	0.1860	0.3256

Table 3 PSNR value comparison of the proposed method on Lena, Barbara and Pirate image with [11, 13, 14]

Method	Lena	Barbara	Pirate
[14]	43.6622	NA	NA
[13]	43.65	46.35	NA
[11]	49.47	49.60	50.80
Proposed method	74.3644	67.7891	62.4682

salt and pepper noise, cropping and scaling. Proposed watermarking also performed well against the attacks.

Table 1 illustrates that watermarked image have good quality with high PSNR value. The main objective of this proposed method is to improve imperceptibility. So, to validate the objective of proposed method, perceptual quality parameter is compared with previously developed scheme [11, 13, 14,]. Table 2 Exhibits the imperceptibility comparison of proposed method with previously developed schemes and proves that proposed watermarking method is excellent in terms of imperceptibility.

6 Conclusion and future scope

This paper proposes an image watermarking method with aim of improving imperceptibility. The robustness of watermarking method is also checked. The proposed image watermarking method consists of block division, entropy and histogram. Some of findings from this paper are as follows:

1. Work related to block entropy and histogram shape is discussed and suggested a new image watermarking method with an objective of improving imperceptibility.
2. Combination of both entropy and histogram improves performance of watermarking scheme. Watermark is inserted into selected blocks instead of whole gray scale image.
3. For block selection, host image is preprocessed with entropy. Image areas with high entropy value are least visible to human which makes our scheme more imperceptible and also improves perceptual quality of watermarked image.
4. The trait of histogram shape is employed for embedding watermark into selected area of host image. Histogram of image is independent of pixel location. So it will help in maintaining resistance under few attacks like scaling.

5. Experimental results exhibit that proposed method has better imperceptibility and robustness is also verified.
6. The robustness of watermarking method can be improved further by employing optimization techniques like genetic algorithm, PSO and neural networks.

References

1. Zargar AJ, Singh AK (2016) Robust and imperceptible image watermarking in DWT-BTC Domain. Int J Electron Secur Digital Forensics 8(1):53–62
2. Panneerselvam M, Divya R, Vijayalakshmi V (2017) Multilevel watermarking technique for securing multibiometric templates using DTCWT and SVD. Int J Image Min 2(3–4):277–291
3. Pande J, Singh BK, Joshi S (2018) Watermarking of audio signals using iris data for protecting intellectual property rights of multiple owners. Int J Inf Technol 10(4):559–566
4. Shaamala A, Abdullah SM, Manaf AA (2011) The effect of DCT and DWT domains on the robustness of genetic watermarking. In: Abd Manaf A, Zeki A, Zamani M, Chuprat S, El-Qawasmeh E (eds) Informatics Engineering and Information Science, ICIEIS 2011. Communications in Computer and Information Science, vol 251. Springer, Berlin, pp 310–318
5. Bashir R, Giri KJ (2018) A block based watermarking approach for color images using discrete wavelet transformation. Int J Inf Technol 10(2):139–146
6. Bedi SS, Chandra MA (2018) Survey on SVM and their application in image classification. Int J Inf Technol 4:1–11
7. Banerjee M, Chaudhuri A, Das S (2018) An improved video keyframe extraction algorithm leads to video watermarking. Int J Inf Technol 10(1):21–34
8. Kannan D, Gobi M (2015) An extensive research on robust digital image watermarking techniques: a review. Int J Signal Imaging Syst Eng 8(1–2):89–104
9. Kasturi R, Schunck BG, Jain R (1995) Machine vision. McGraw-Hill, New York City
10. Kiran KG (2015) Watermark embedding and extraction using histogran shifting and butterworth filtering. Int J Adv Res Comput Sci Softw Eng. 5(5):1481–1487
11. Xiang Y, Natgunanathan I, Zong T (2014) Histogram shape based robust image watermarking method. IEEE ICC 2014-communication and information system security symposium, pp. 878–883.
12. Xiang Y, Natgunanathan I, Guo S, Zhou W, Beliakov G, Zong T (2015) Robust histogram shape-based method for image watermarking. IEEE Trans Circuit Syst Video Technol 25(5):717–729
13. Zhu T, Yang G, He X (2013) A geometrical attack resistant image watermarking algorithm based on histogram modification. Multidimens Syst Signal Process 26:291–306
14. Hou W, Wang S (2009) A robust watermarking algorithm based on histogram. IWISA, Qingdao, pp 453–456
15. Alam MZ, Umayya Z, Khan S, Ahmad F, Ahmad M (2018) An image encryption approach using particle swarm optimization and chaotic map. Int J Inf Technol 10(3):247–255
16. Gao X, Li X, Tao D, Deng C (2010) Local histogram based geometric invariant image Watermarking. Signal Process 90(12):3256–3264
17. Bailey K, Leeney M, Curran K, Lusson F (2012) A novel approach to digital watermarking exploiting colour spaces. Signal Process 93:1268–1294
18. Kim H-J, Huang J, Xiang S (2007) Histogram-based image hashing scheme robust against geometric deformations. Proceddings of the 9th workshop on Multimedia and Security. New York City, ACM, pp 121–128
19. Goel N, Singh G (2016) Entropy based image watermarking using discrete wavelet transform and singular value decomposition. 2016 IEEE International Conference on Computing for Sustainable Global Development, New Delhi, pp 2700–2704
20. Hu X, Wang D (2015) A histogram based watermarking algorithm robust to geometric transformations. ICECEE, Jinan, pp 773–779
21. Fotopoulos V, Xenos M, Skodras AN, Chrysochos E (2012) Hybrid watermarking based on chaos and histogram modification. Signal Image Video Process. 8:843–857
22. Huang H-N, Chen C-J, TsengK-K TuS-Y, Chenn S-T (2013) Adaptive audio watermarking via optimization point of view on the wavelet-based entropy. Digital Signal Process 23:971–980
23. Zhang Y, Yang C, Li W, Yang Q (2012) Information entropy used in digital watermarking. IEEE Symp Photon Optoelectron (SOPO) 2012:1–4
24. Dutta A, Kumar S (2016) A novel Spatial domain technique for digital image watermarking using block entropy. IEEE Conf Recent Trends Inf Technol (ICRTIT) 5:1–4
25. Huertas R, Gebejes A (2013) Texture characterization based on grey-level co-occurrence matrix. Proc Conf Inf Manag Sci. 1:375–378
26. Fabien A. P. Petitcolas (2018) Public-domain test images for homeworks and projects. [Online]. https://homepages.cae.wisc.edu/~ece533/images/. Accessed 28 Aug 2018
27. Woods RE, Eddins S, Gonzalez RC (2018) ImageProcessingPlace.com. [Online]. http://www.imageprocessingplace.com/root_files_V3/image_databases.htm. Accessed 28 Aug 2018