Information Sciences 222 (2013) 323–342

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Local Shannon entropy measure with statistical tests for image randomness

Yue Wu [a,*], Yicong Zhou [b], George Saveriades [a], Sos Agaian [c], Joseph P. Noonan [a], Premkumar Natarajan [d]

[a] Department of Electrical and Computer Engineering, Tufts University, 161 College Ave., Medford, MA 02155, USA
[b] Department of Computer and Information Science, University of Macau, Ave. Padre Tomás Pereira, Taipa, Macau, China
[c] Department of Electrical and Computer Engineering, University of Texas at San Antonio, One UTSA Circle, San Antonio, TX 78249, USA
[d] Raytheon BBN Technologies, 10 Moulton Street, Cambridge, MA 02138, USA

ARTICLE INFO

Article history:
Received 24 March 2011
Received in revised form 25 July 2012
Accepted 30 July 2012
Available online 7 August 2012

Keywords:
Image encryption
Shannon entropy
Image randomness
Hypothesis test

ABSTRACT

In this paper we propose a new image randomness measure using Shannon entropy over local image blocks. The proposed local Shannon entropy measure overcomes several weaknesses of the conventional global Shannon entropy measure, including unfair randomness comparisons between images of different sizes, failure to discern image randomness before and after image shuffling, and possible inaccurate scores for synthesized images. Statistical tests pertinent to this new measure are also derived. This new measure is therefore both quantitative and qualitative. The parameters in the local Shannon entropy measure are further optimized for a better capture of local image randomness. The estimated statistics and observed distribution from 50,000 experiments match the theoretical ones. Finally, two examples are given, applying the proposed measure to image randomness among shuffled images and encrypted images. Both examples show that the proposed method is more effective and more accurate than the global Shannon entropy measure.

1. Introduction

Since the information age began in the late 1970s, the digital world has kept evolving on a nearly daily basis. More particularly, the past 10 years have seen an impressive growth of capabilities of electronic devices as well as their usage in virtually all walks of life (i.e. smartphones, digital music players, home robotic devices, electronic readers, etc.). These devices highlight the fast increase in computational and storage facilities of modern electronics. Compared to the rapid development of electronic devices and computer computational capacities, contemporary data encryption technologies are not very different from those of 10 years ago: many data encryption algorithms in use 10 years ago are still in use today, such as the data encryption standard (DES) [2] dating from 1976, the Blowfish cipher [7] from 1993, the Twofish [46] cipher from 1998, and the advanced encryption standard (AES) [3] from 1998. Although shortcomings of these methods on bulk data, such as digital images and digital videos, have been pointed out [61], these old algorithms still dominate encryption methods at all levels (individuals, organizations, companies and governments).

Image encryption has recently become a fertile research area. Many new image encryption algorithms or methods have been proposed, e.g. chaotic system based image ciphers [6,12,15,16,22,28,29,37,40,42,54,55,63,64], SCAN language based algorithms [13,14], transform based algorithms [35,38,49,60,65]. The goal of image encryption is to turn an input image, commonly referred to as *plaintext*, into an unrecognized or unintelligent image, referred to as *ciphertext*, using a predetermined method, which is called an *image cipher*. For adversaries without plaintext knowledge, an image cipher works like

* Corresponding author. Tel.: +1 617 627 3217.
E-mail address: ywu03@ece.tufts.edu (Y. Wu).

0020-0255/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2012.07.049

a symbol source generating pixels in ciphertext. Since the completely random source achieving the maximum randomness has a uniform distribution, it is desirable that an image cipher has an indistinguishable distribution. Otherwise, the image cipher is insecure as patterns can be identified through the observation of a sufficiently large number of encrypted images [11,32,33,56].

Image randomness can be measured using a variety of methods, such as histogram analysis [6,12,16,22,28,29,35,37,40,42,54,55,57,60,63,64], global Shannon entropy measure [6,12,42,55,64,66], adjacent pixel correlations [6,12,16,35,42,57,64,66]. One major drawback of these conventional techniques is that they provide quantitative rather than qualitative measures. However, it is qualitative measures that make it is possible to distinguish patterned data from random-like data. In contrast, many statistical tests that provide quantitative measures (e.g. the Kolmogorov test [50], poker test [50], gap test [50], autocorrelation test [50], diffusion randomness test [27], and available test suites such as FIPS 140-1 [1] and 140-2 [4]) are designed for either a stream or a block cipher, which is built for one dimensional bit-stream rather than a two dimensional image. These methods are therefore not directly applicable to image data.

Although the importance of statistical tests for image randomness is obvious, little work has been done on this particular topic. Refs. [34,62] discussed a randomness measure defined on image edges; however, it is still a quantitative measure which only gives a randomness score. Statistical tests for the number of changing pixel rate (NPCR) and the unified average changing intensity (UACI) [6,12,16,35,54,55,57,64,66], two measurements on the changing rate of encrypted images, have been proposed recently in [59], but they are made for testing randomness between two images rather than on the randomness of one image.

In this paper, we develop new statistical tests for image randomness based on the local Shannon entropy measure, which is a generalization of conventional Shannon entropy. The remainder of the paper is organized as follows: Section 2 gives a brief review on Shannon entropy, the central limit theorem and random number generators in cryptography; Section 3 introduces a random image generator model, and derives the mean and variance of Shannon entropy for random images; Section 4 defines the local Shannon entropy measure and statistical tests for random images, and optimizes parameters of the local Shannon entropy measure to attain the best localization capacity; Section 5 compares the theoretical statistics and distributions with those observed from a large scale simulation with 50,000 random images; Section 6 presents possible applications of the proposed method for image shuffling and image encryption; and Section 7 concludes the paper.

2. Preliminaries

2.1. Shannon entropy measure and properties

Shannon entropy [47], named after Claude Shannon, was first proposed in 1948. Since then, Shannon entropy has been widely used in the information sciences. Shannon entropy is a measure of the uncertainty associated with a random variable. Specifically, Shannon entropy quantifies the expected value of the information contained in a message. The Shannon entropy of a random variable X can be defined as in Eq. (1), where P_i is defined in Eq. (2) with x_i indicating the ith possible value of X out of n symbols, and P_i denoting the possibility of $X = x_i$.

$$\mathrm{H}(X) = \mathrm{H}(P_1, \ldots, P_n) = -\sum_{i=1}^{n} P_i \log_2 P_i \tag{1}$$

$$P_i = \Pr(X = x_i) \tag{2}$$

Shannon Entropy attains, but is not limited to, the following properties:

(a) Bounded: $0 \leqslant \mathrm{H}(X) \leqslant \log_2 n$
(b) Symmetry: $\mathrm{H}(P_1, P_2, \ldots) = \mathrm{H}(P_2, P_1, \ldots) = \cdots$
(c) Grouping [45]: $\mathrm{H}(P_1, \ldots, P_n) = \mathrm{H}(P_1 + P_2, P_3, \ldots, P_n) + (P_1 + P_2)\,\mathrm{H}(P_1/(P_1 + P_2), P_2/(P_1 + P_2))$

In the context of digital images, an $M \times N$ image X can be interpreted as a sample from an L-intensity-scale source that emitted it. As a result, we can model the source symbol probabilities using the histogram of the image X (the observed image) and generate an estimate of the source entropy [23]. For example, an 8-bit gray image allows $L = 256$ gray scales from 0 to 255. Additionally, denote the number of pixels within image X at pixel intensity scale l as n_l. Then

$$P_l = \Pr(X = l) = n_l / T \tag{3}$$

where $l \in \{0, 1, \ldots, L-1\}$ denotes the intensity scale and $T = M \times N$ is the total number of pixels in image X. Therefore, the Shannon entropy score of image X can be calculated as shown in Eq. (4).

$$\mathrm{H}(X) = -\sum_{l=1}^{L-1} P_l \log_2 P_l = \sum_{l=0}^{L-1} \frac{n_l}{T} \log_2 \frac{T}{n_l} \tag{4}$$

The theoretical maximum of the Shannon entropy score for an L symbol source is $\log_2 L$, when each symbol is equally likely distributed, i.e.

$$P_0 = P_1 = \cdots = P_l = \cdots = P_{L-2} = P_{L-1} = 1/L \tag{5}$$