2009 REU in Telematics and Cyber Physical Systems

Digital Document Authentication

Faculty Mentors: Dr. Syed Masud Mahmud and Dr. Feng Lin
Grad Student Mentor: Shankar Ganesh

Malek Musleh, University of Michigan, Dearborn, Michigan

Abstract:

The goal of this paper is to illustrate a new method of certifying and authenticating digital documents. This method aims to exploit the distinctive characteristic of a paper document's grain structure to develop a unique paper signature to certify the document's authenticity. The grain structure of one sample of paper, will never have quite the same characteristics of another sample paper, even if both samples are of the same color, type, or originated from the same source. The documents are compared digitally, requiring the authenticator to have a digital image of the paper document in question as well as a digital image of the original document. The intent of this method is to apply a "fingerprint" signature to each certifying document in order to safeguard against counterfeiting. This certification method is highly invulnerable to the main forms of counterfeiting, copying and spoofing, as replicating or reconstructing a paper's grain structure becomes quite difficult. Figure 1 illustrates a type of copy attack.

Introduction:

In this new age of industrialized equipment and computing, document security has become an area of concentrated focus, as developing technology is able to provide the means for document forging and replication. As a result, several different methods and tools have been developed to safeguard the authenticity of documents, such as Watermarking, Digital Watermarking, Moirés Patterns, and digital signatures.

Background Material:

Digital Watermarking- Digital watermarking is the process of embedding certain information into a digital signal, in the format

Figure 1: Example of Copy Attack

Moiré Patterns- A moiré pattern is an interference pattern when two grids are overlaid at a certain angle, or when they have slightly different mesh sizes.

Digital Signatures- A digital signature is a type of asymmetric cryptology. The notion of a digital signature is derived from handwritten signature that is used to signify validation of the document's content with the author's signature. In using one of several different public-key encryption algorithms, such as RSA or DSA.

Description of Work:

[1]-Upon selecting the regions of extraction, a process of unifying the illumination is applied to eliminate any non-uniformity illumination that may exist in the image.

[2]- This is followed by applying a *kuan filter* to initially remove any *'speckle'* noise that may reside in the digital image. This assists in removing some of the outlier bright pixels that are farther away from the ROI, but is not as effective in removing extraneous noisy pixels that may be closer to the boundaries of the ROIs.

[3] – Next, a special type of image averaging filter is subsequently applied. In particular, this type of Averaging Filter is known as a Median Filter,

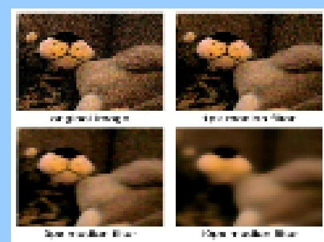
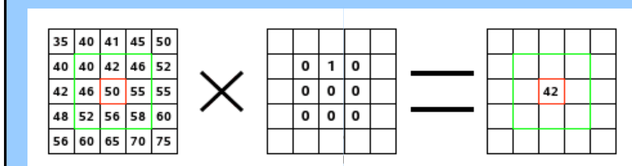


Figure 2: Effect of Applying Median Filter on Noisy Image

[4]-Next, an edge detection algorithm is applied to determine the boundaries of the ROI to complete the extraction process. The type of edge detection algorithm used is known as the *'sobel'* edge detection.

[5]- Next, the image may require some sharpening to compensate or remove some image blurring that may result from the smoothing operation of the filter. In enhancing the contrast of the image's pixels, discrete ROI boundaries can be obtained. To sharpen the image's pixels, a convolution kernel is applied. Figure 3 illustrates the operation of a convolution kernel on a digital image.



el

[6]- Once the coordinates of the corresponding ROI's edges are obtained, the corresponding sub image is then extracted from the original captured image for comparison. Figure 3 depicts a sample paper document with indicated ROI.

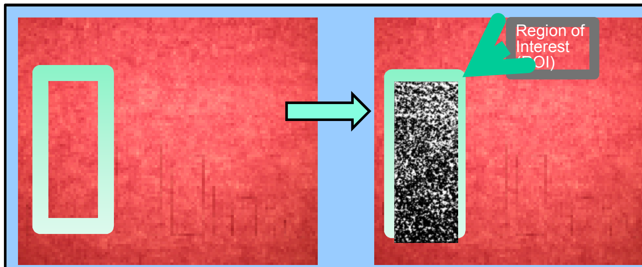


Figure 4: Extraction of ROI from Original Image

[7]-To numerically compare the two images; the statistical method of ***cross correlation*** is used. Cross correlation is used to assign a unique single number (between the ranges of -1 and 1) to the correlation between the two images.

Results and Discussions:

In the comparing digital images of different type and different sample with all possible combination comparisons between them, the results exhibit similar results. Images of the same exact type and sample but different copy exhibited a very high correlation value (e.g. >= 95%), therefore correctly validating the images' authenticity. In regards to other image comparisons, the correlation value rarely exceeds that of 80%, Figure 5 illustrates the results.

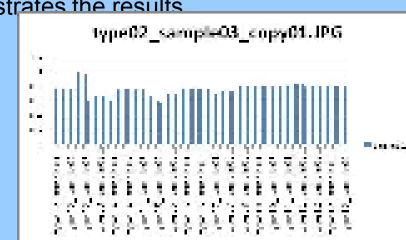


Figure 5: Correlation Chart of Largest Compared ROI

Conclusions:

Due to a lack of complete perfectness in the extraction process, it is difficult to effectively compare pixels utilizing a method such as cross correlation that is heavily dependent on individual pixels. Rather, it may seem appropriate to select a mathematical model that is more generalized in its comparison scheme..

A similar field worth investigating would be fingerprint analysis and comparison. The notion of utilizing the grain structure of a paper document in ensuring its authenticity can be related to the field of fingerprint analysis.

References:

1- Feng Lin, Robert D. Brandt, Stephen Lacy.
A Document Certification and Authentication System.
2- Alasdir McAndrew, *An Introduction to Digital Image Processing with MATLAB*
3- Rafael Gonzalez and Richard E. Woods, *Digital Image Processing.* Addison-Wesley, 2nd Edition, 2002.
4- Yasmina Chitti, *Detection of Small Local Intensity Changes in CCD Images with Nonuniform Illumination and Large Dependent Noise.* March 1997.
5-http://manual.gimp.org/en/plug-in-convmatrix.html