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 of audio, video, or picture. Figure 1 illustrates a type of copy attack. Digital signatures- A digital signature is a type of asymmetric cryptography. 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.

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.

Figure 2: Effect of Applying Median Filter on Noisy Image

Figure 3: Application of 3X3 Convolution Mask for Pixel

Figure 4: Extraction of ROI from Original Image

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 
4- Yasmina Chitti, Detection of Small Local Intensity Changes in CCD Images with Nonuniform Illumination and Large Dependent Noise. March 1997. 
5- Malek Musleh, An Introduction to Digital Image Processing with MATLAB 
6- Regional Intensity Differences
7- Cross Correlation
8- Averaging Filter
9- Median Filter
10- 3X3 Convolution Mask
11- Convolution Kernel
12- 42
13- el
14- Malek Musleh, University of Michigan, Dearborn, Michigan
15- 2009 REU in Telematics and Cyber Physical Systems
16- Digital Document Authentication
17- 2009 REU in Telematics and Cyber Physical Systems