Multimedia Document Authentication using On-line Signatures as Watermarks

Anoop M. Namboodiri and Anil K. Jain
Department of Computer Science and Engineering
Michigan State University
East Lansing, MI 48824
{anoop, jain}@cse.msu.edu

ABSTRACT

Authentication of digital documents is an important concern as digital documents are replacing the traditional paper-based documents for official and legal purposes. This is especially true in the case of documents that are exchanged over the Internet, which could be accessed and modified by intruders. The most popular methods used for authentication of digital documents are public key encryption-based authentication and digital watermarking. Traditional watermarking techniques embed a pre-determined character string, such as the company logo, in a document. We propose a fragile watermarking system, which uses an on-line signature of the author as the watermark in a document. The embedding of a biometric characteristic such as signature in a document enables us to verify the identity of the author using a set of reference signatures, in addition to ascertaining the document integrity. The receiver of the document reconstructs the signature used to watermark the document, which is then used to verify the author's claimed identity. The paper presents a signature encoding scheme, which facilitates reconstruction by the receiver, while reducing the chances of collusion attacks.

Keywords: Fragile watermarking, Document authentication, Biometrics, On-line signature verification

1. INTRODUCTION

Digital documents that are exchanged over the Internet can be accessed or modified by a malicious user with relative ease. This creates an important security concern while exchanging multimedia data over the Internet. Multimedia data contains information in the form of audio, video, still images, etc. Large amounts of multimedia data are being made available in many digital repositories such as newspaper and television web sites and museum databases, which archive historic documents. This increases the need for authentication and verification of document integrity for users of such data. One of the well-known methods used for authentication of digital documents is the public key encryption-based authentication.[1] However, the encryption-based method is not suitable for widespread distribution of a document since it needs to be decrypted by each recipient before using it or additional data should be tagged along with the document. An alternate approach uses digital watermarking[2] to ascertain the source/origin of the document, where a signature string is embedded in the document in such a way that the contents of the document are not altered. Watermarking can also be used in conjunction with encryption-based authentication techniques to provide an additional level of security in document authentication.

Traditional watermarking techniques embed a character string, such as the name of the author in a document. However, this does not guarantee the document source, since anyone can watermark a document with a particular name. The use of a biometric trait, such as signatures, can increase the utility of watermarking techniques for authentication. In addition to the long-standing acceptance of signatures for (paper) document authentication, watermarking techniques using signatures can assure that the document was not tampered with after it was signed. The embedding of a biometric characteristic such as signatures in a document also enables us to verify the signature of the author, thereby reducing the chance of a forgery.

Watermarking techniques have been studied extensively in the past. Petitcolas et al.[3] provide a comprehensive survey of digital watermarking techniques. The most common variety of watermarking technique involves robust watermarking for copyright protection.[4] However, for the purpose of authentication, we need to assure that a digital document has not been tampered from the time it was created and signed by the author to the time it was received at the destination. The specific problem of watermarking using biometric traits has been studied in

the context of authenticating a biometric template by Jain et al.[5] A detailed description of various data hiding techniques for authentication and other applications can be found in Wu and Liu.[2]

Petitcolas et al.[3] classify the various information hiding techniques according to their use and properties (see figure 1). The class of watermarking techniques suitable for document authentication fall under the category of fragile watermarking techniques. The use of a biometric trait to watermark a document introduces an additional processing step at the receiving end; that of verification of the biometric trait against the claimed identity of the author. This means that any coding and embedding scheme should be evaluated in terms of the robustness/fragility of the watermark as well as the verification performance of the decoded biometric trait.

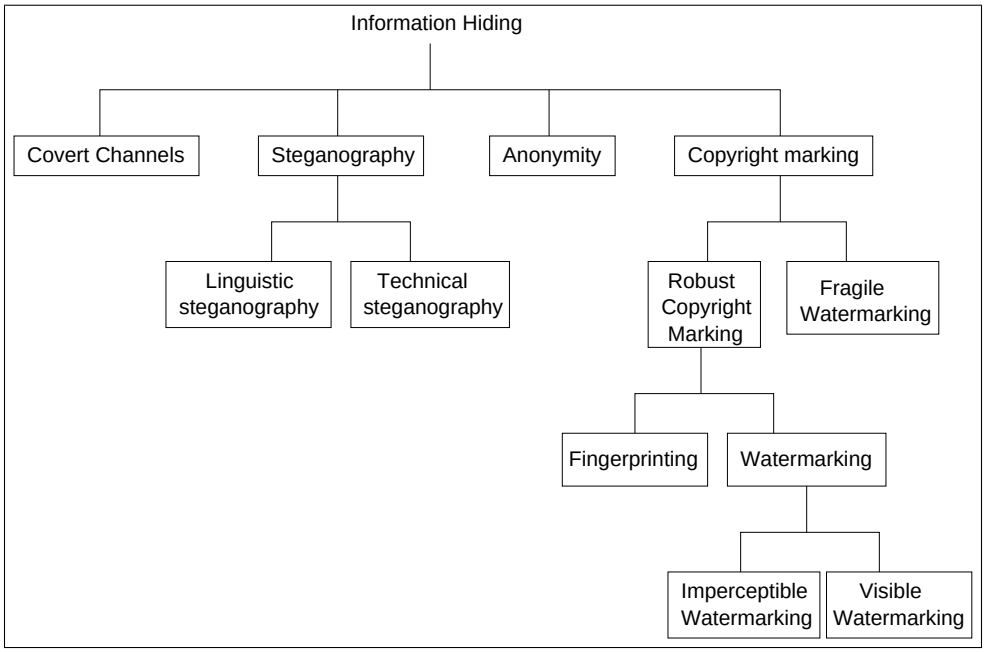


Figure 1. Classification of information hiding techniques by Petitcolas et al.[3]

Kundur and Hatzinakos[6] proposed a fragile watermarking technique for wavelet compressed still images for the purpose of document authentication. Yeung and Mintzer[7] proposed a fragile watermarking system for image verification. A modification of the above algorithm was used by Yeung and Pankanti[8] for the specific purpose of authenticating biometric data. Figure 2 shows a schematic diagram of a fragile watermarking authentication system. The diagram contains two modules. The fragile watermark embedding module accepts a document image (I) and a watermark image, W, and inserts W into I to generate the watermarked image ω. The insertion procedure is based on a secret key, which is known (only) to the sender and receiver of the document. The fragile watermark detection module at the receiver's end uses the secret key to extract the watermark, W', from the received document, ω'. If W' is identical to W, then the document is declared to be authentic.

2. DOCUMENT AUTHENTICATION

Authentication of a document image using watermarking should ensure that the document has not been altered from the time it was created and signed by the author to the time it was received at the destination. This means that any alteration of the document, however small, should be detectable during the watermark extraction stage. For the purpose of detecting tampering, it is desirable for a fragile watermarking system to have the following properties:

1. The authentication system should be able to detect areas of document image which have been altered after watermarking, in addition to detecting whether the document has been altered at all.

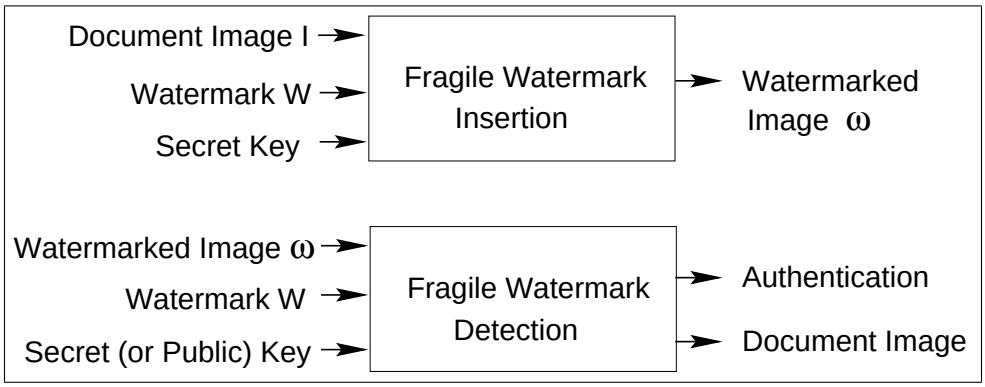


Figure 2. Schematic diagram of a fragile watermarking authentication system.

2. The watermark should be invisible to a person who does not know the secret key and it should be secure against attacks to extract the watermark.

3. The watermarking process should not perceptually alter the document image.

To accomplish the first goal, the watermark detection scheme should compute a watermark function $WM()$ for every pixel of the document image and compare the function value against a reference value (typically the watermark image). To detect any altered pixels, most verification (fragile) watermarking algorithms (e.g., Yeung and Mintzer[7]) use a binary image of the same size as the host image as watermark. The watermark image is any binary image, whose pixels could be shuffled to reduce the chances of watermark detection (see Voyatzis and Pitas[9]) using techniques such as vector quantization. This technique was used by Yeung and Pankanti[8] for watermarking fingerprint images. In addition, the pixel values in the host image should be altered as little as possible to preserve the appearance of the host document.

3. DOCUMENT AUTHENTICATION USING ON-LINE SIGNATURES

We propose to use the on-line signature[10] of the author, captured at the time of signing the document, to generate a watermark image. The use of a biometric characteristic such as signature as the watermark image, provides an added level of security in the authentication process. In addition to ensuring that the document has not been altered, one could also use the extracted watermark, the on-line signature, to verify the identity of the claimed author. Moreover, the need of a secret watermark image is avoided by using the signature as a watermark. The use of signature has the advantage over other biometric characteristics that it has a long history of being accepted for document authentication.

Figure 3 gives a schematic diagram of the watermark embedding and detection stages of our algorithm. We use the on-line signature to generate a binary image, which is used as the watermark image (see section 3.2). Figure 4 shows a document image, which is watermarked using an on-line signature. The document image was scanned from a conference announcement poster.

3.1. On-line Signature Verification

Handwritten signatures are commonly used to certify the contents of a document or to authenticate legal transactions. Signature verification is usually done by visual inspection. In automatic signature verification, a computer takes over the task of comparing two signatures to determine if the similarity between the signatures exceeds some pre-specified threshold.

Handwritten signature is a well-known biometric attribute. Other biometric attributes, which are commonly used for authentication include iris, hand geometry, face and fingerprints (See Jain et al.[11]). While attributes like iris and fingerprints do not change over time and thus have very small intra-class variation, they require special

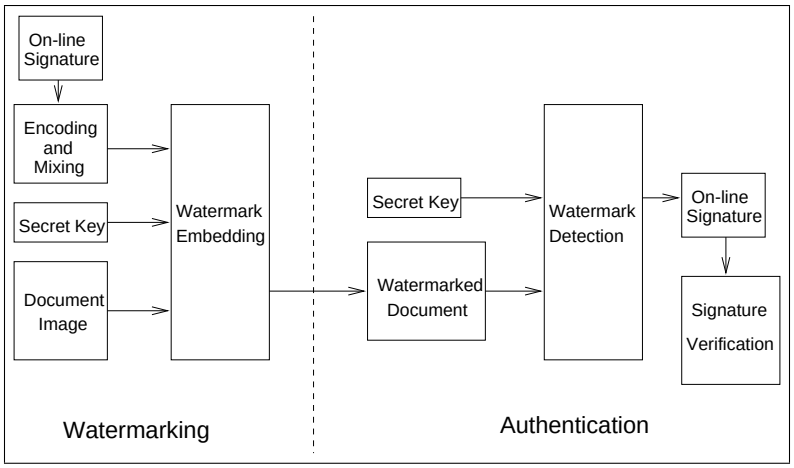
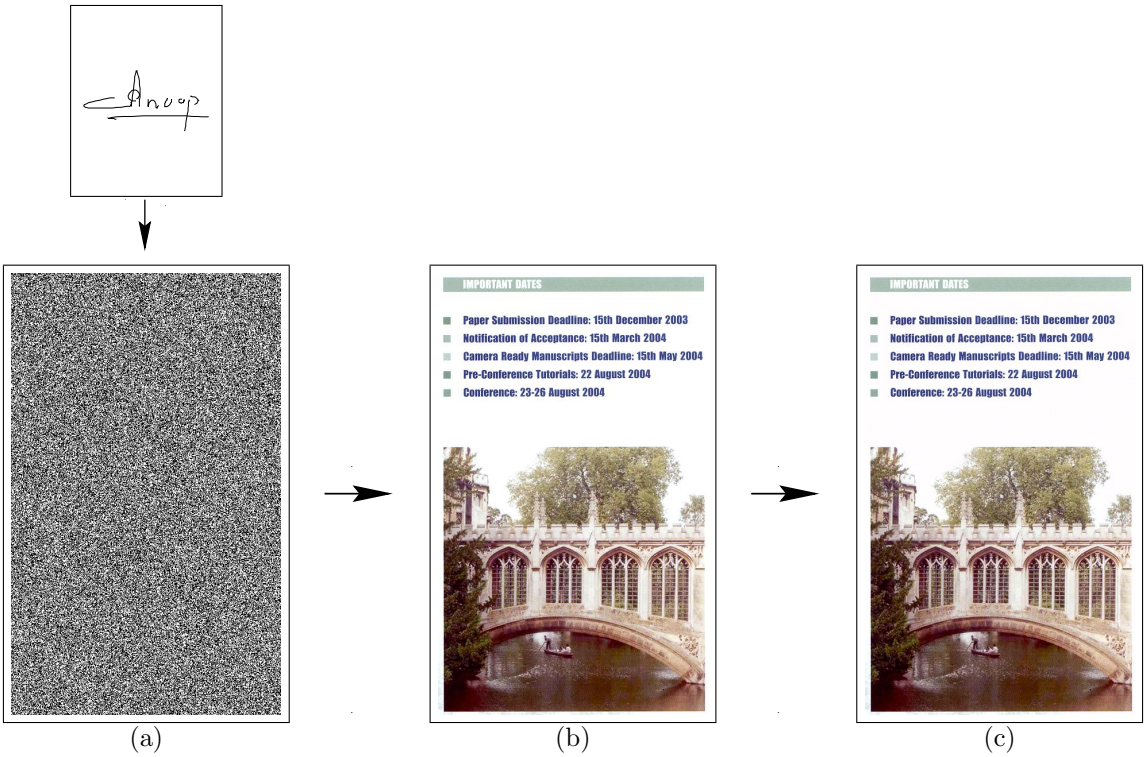


Figure 3. Schematic diagram of a fragile watermarking and authentication system.

and relatively expensive hardware to capture the biometric data. An important advantage of the signature over other biometric attributes is that it has been traditionally used in authenticating documents and hence is socially accepted.

On-line signature captures the dynamics of signing in addition to the spatial information contained in an off-line signature. This enables us to use the speed and direction of movement of the pen tip along with its spatial co-ordinates in matching. Devices such as Tablet PCs and PDAs allow us to input data using a pen



(a) (b) (c)

Figure 4. Watermarking using on-line signature: (a) binary watermark image generated from an on-line signature. (b) document image, which is watermarked using (a), resulting in the image shown in (c).

or stylus and they can capture the dynamic (i.e., temporal and pressure) information when a user signs on the screen. The dynamic information in on-line signatures makes it extremely difficult to forge a signature. Figure 5 shows part of a signature by the genuine user and a forger, who was copying the signature from an off-line sample on a paper. The temporal order of the strokes of the signature is indicated in paranthesis. The direction of drawing of the individual strokes is denoted by an arrow, and the dots on the lines represent sample points. Note that the distance between two sample points is directly proportional to the speed of writing as the samples are collected at equal intervals of time. We can observe that the forged signature, although similar in spatial appearance, is very different when we consider the order and direction of drawing the strokes, and the speed of writing at the corresponding spatial locations.

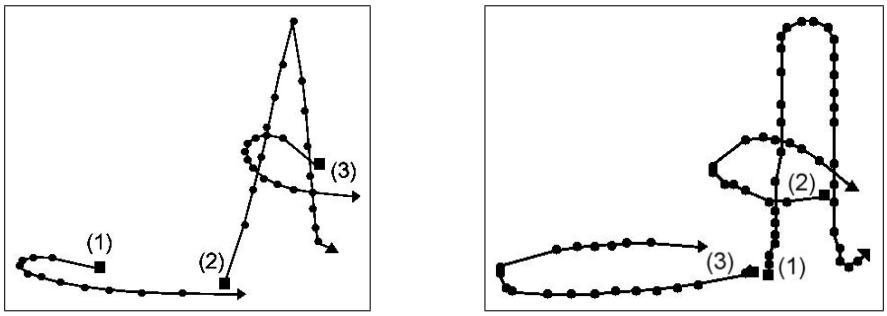


Figure 5. Genuine and forged signatures: (a) on-line signature by genuine user, and (b) an attempt to forge (a) by copying from an off-line sample. The stroke order is indicated in parenthesis. The dots on the strokes represent sample points and arrows represent the writing direction.

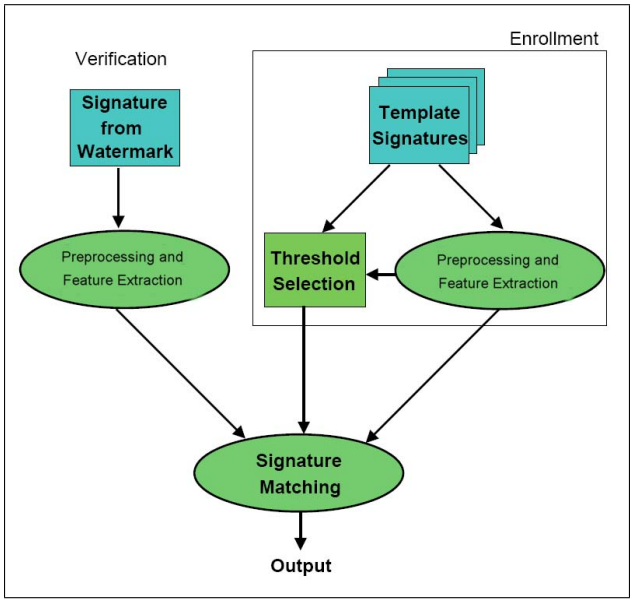


Figure 6. Schematic diagram of a signature verification system.

Figure 6 shows a schematic diagram of a signature verification system.[10] During enrollment of a new user, a set of reference signatures is provided by the user. This data is saved in a database together with a unique identifier (ID) for the user. During the verification stage, the signature, which is extracted from the watermarked image is input to the verification module, along with the claimed identity of the author. The signature is then compared to each of the reference signatures which are retrieved from the database based on the claimed identity (ID). This signature is accepted as genuine or rejected as a forgery, based on the matching

3.2. Generating the Watermark Image

The on-line signature of the author, collected using a CrossPad® , is re-sampled to ensure that consecutive sample points along the signature are atmost 8 pixels apart. A typical signature has around 200 sample points in our experiments. Each sample point is encoded using a single byte representing its distance from the previous sample point. The signature is then converted to a bit stream that is repeated to form an image of the same size as the document image. A toral automorphism * is then applied to the watermark image[9] to make the watermark image random. Figure 7 shows the generation of the watermark image from an on-line signature.

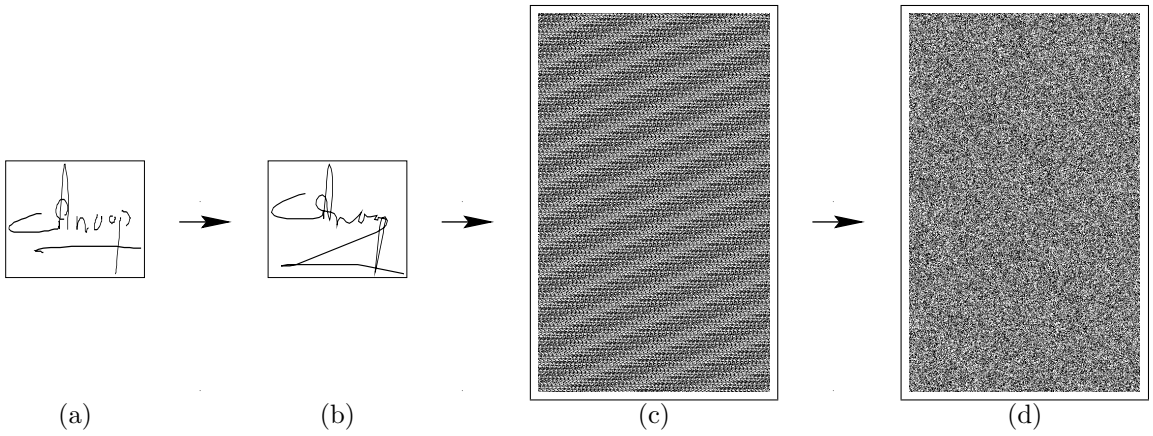


Figure 7. Generation of watermark image from an on-line signature: (a) on-line signature, (b) strokes in (a) are connected together to form a single stroke, (c) the binary image obtained from (b). The binary image in (b) is shuffled to get the watermark image in (d).

3.3. Embedding the Watermark

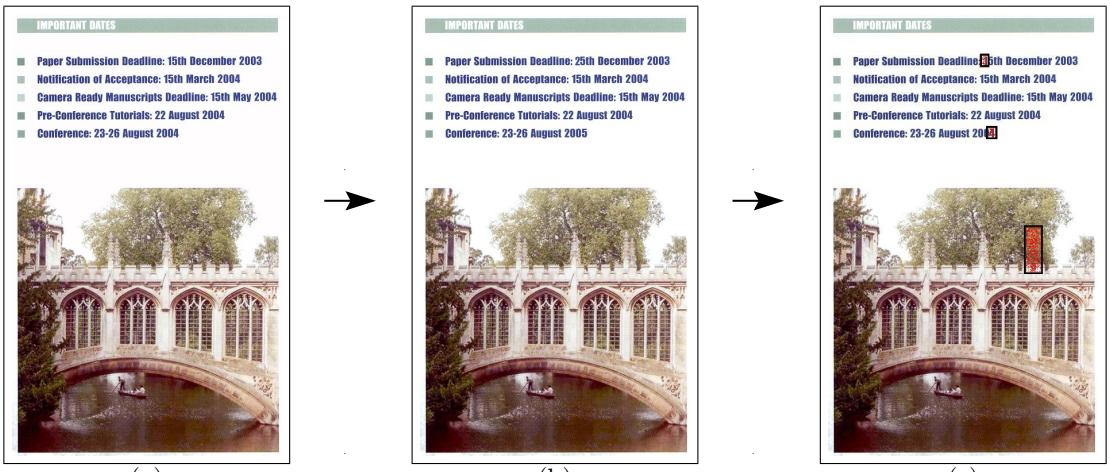
The process of embedding the watermark image into the host image (document image) should ensure that the pixel values are modified by the least amount possible to avoid any perceptual change in the document. The watermark function we use is generated using a pseudo random number generator. A $mod1$ operation, applied to the random sequence of length 256 yields a mapping from the gray values of the document image to a binary number. This serves as the watermark function, and is controlled by the secret key, which is used as a seed to generate the random sequence.

The watermark function at each pixel of the document is computed and compared against the value of the watermark image. If the values match, the pixel in the document is left unchanged. If they do not match, the pixel value is modified by a very small amount, such that the watermark function and the binary pixel value of the watermark image are identical. One might notice that the change in value required might be quite high in case when the binary random sequence contains a series of *zeros* or *ones*. We avoid this problem by modifying the random sequence, so that there are atmost 8 consecutive *zeros* or *ones*. Our watermark embedding is similar to the one proposed by Yeung and Pankanti.[8]

*A toral automorphism is a bijection from a rectangular array to another array of the same size[9]

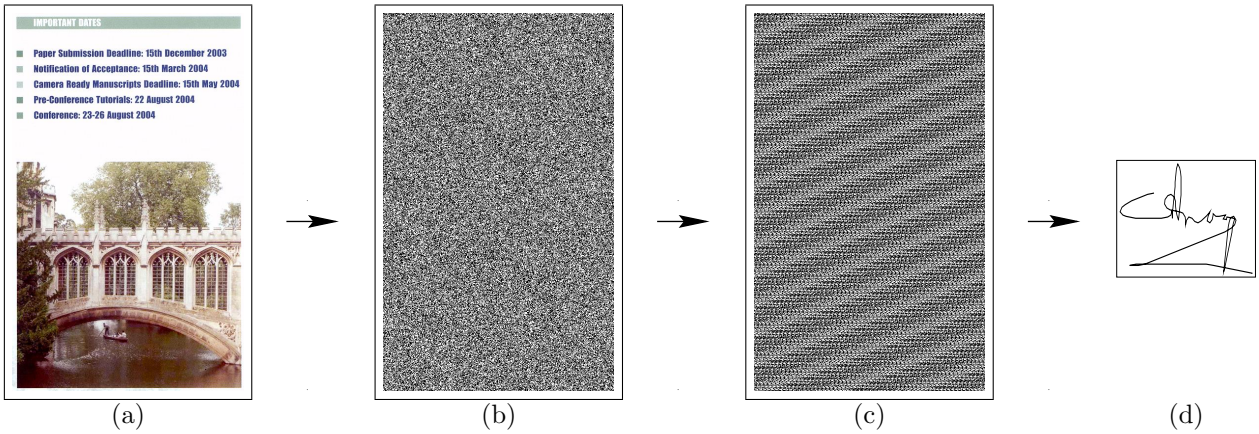
3.4. Watermark Detection and Authentication

During the detection stage, the watermark image is recovered using the watermark function, generated using the secret key. Once the watermark image is recovered, a reverse mapping of the mixing function used during the encoding stage will yield back the embedded signature. Note that there are multiple copies of the input signature in the watermark image (176 copies of the signature in the example in figure 7). The corresponding bits in different signatures included in the watermark image are then compared to see if they agree. If the bits agree in all the signatures, we conclude that the pixel is unaltered. Note that there should be at least two instances of the signature in the document image for this approach to work. To locate the pixels that were altered, we need to recover the original watermark image at the receiving end. We use the majority among the corresponding pixel values of the different signatures as an estimate of the original signature string. Figure 8 shows a watermarked document, which was modified after watermarking and the result of the watermark extraction process. The pixels where tampering was detected are shown in red. The on-line signature is then reconstructed from the watermark image. Figure 9 shows a watermarked document image and the recovered on-line signature.



(a) (b) (c)

Figure 8. Detecting tampered locations in a document image: (a) watermarked document image, (b) image in (a) that has been modified at three locations. The result of watermark detection is given in (c). Note that regions where a change is detected are shown in boxes.



(a) (b) (c) (d)

Figure 9. Recovering the embedded signature: (a) watermarked document image, (b) watermark image extracted from (a), (c) binary image obtained by the inverse shuffling function, and (d) the on-line signature recovered from (c).

Once the integrity of the document is established, the extracted signature is used for verification of the author's identity. The signature matching algorithm reported in Jain et al.[10] was used for this purpose. One may note that, even in the cases where the integrity detection fails due to the unavailability of multiple signatures in the watermark image, the signature verification stage acts as an additional level of security.

4. EXPERIMENTAL RESULTS

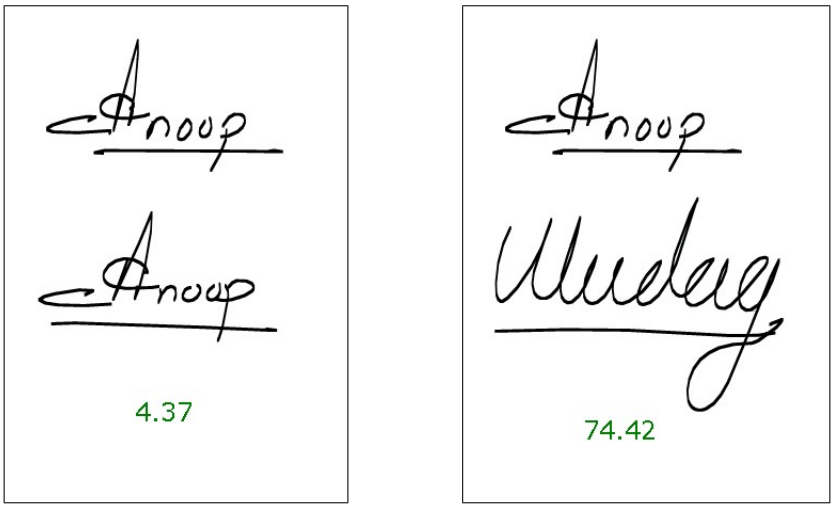
The watermark-based authentication system was used to detect various types of tampering in a variety of documents. We scanned 15 different documents from different magazines and brochures using a flatbed scanner at a resolution of 150 *dpi*. Figure 10 shows a set of 4 document images which were watermarked and then tampered at different locations.

(a) (b) (c)

Figure 10. Tamper detection results: (a) watermarked document image, (b) tampered image constructed from (a), (c) tamper detection results. Pixels where a change is detected are highlighted with dots.

The pixels where a change is detected are highlighted with dots in figure 10(c). The fourth row in figure 10 shows a document image, where the tampering is very subtle (accent sign in the word décor was erased and only 5 pixels were altered). Our watermark detection algorithm missed the tampering. This is due to the fact that

the modified gray levels of the 5 pixels in the tampered image yield the same value of the watermark function $WM()$, as the un-altered pixels. However, this was the only case in 15 document images, each tested 10 times with different number of pixels modified (a total of 150 experiments), where a change of more than three pixels went undetected by the watermark extraction algorithm.



(a) (b)

Figure 11. Matching scores for a genuine and imposter signatures: (a) matching of two signatures by genuine user, and (b) matching scores for an imposter.

We tested the recognition accuracy of the signatures recovered from the document images on a set of $1,000$ signatures collected from 100 users. Of the 10 signatures collected from each user, 3 were used as template signatures and 7 were used for testing. A signature retrieved from a document is compared against every user (100) in the database. The matching score for a particular user is computed as the minimum of the matching scores of the individual template signatures for that user. The user with the smallest matching score is identified by the algorithm as the signee of the document. Figure 11 shows the matching scores for two sets of signatures, one pair by the same user and the second from two different users. The matching threshold computed from the template signatures was 5.0. Figure 12 shows the ROC curve for the signature matching algorithm for the test described above. Note that the *x-axis* is plotted in logarithmic scale. The equal error rate of the signature matching algorithm was 93.2%.

5. CONCLUSIONS AND FUTURE WORK

The paper proposed a fragile watermarking algorithm, where a document image is embedded with an on-line signature of the author. The algorithm can retrieve the embedded signature at the receiving end, and detect changes in the document at the same time. The retrieved signature can then be used for verifying the identity of the author. Results of authentication, carried out on a set of 15 document images, each tested for 10 different cases of alterations, demonstrate the ability of the algorithm to detect changes. The signature recognition algorithm achieved an equal error rate of 93.2% on a database of 100 users and $1,000$ signatures.

We are currently working on analyzing the robustness of the signature recovery. The algorithm will be tested with varying amount of alterations in a watermarked image. In addition to the correctness of the recovered signature, the effect of changes in documents on signature matching will be studied in detail. Finally, possible modifications of the watermark embedding algorithm for enhancing the detection performance for minor changes will be explored.

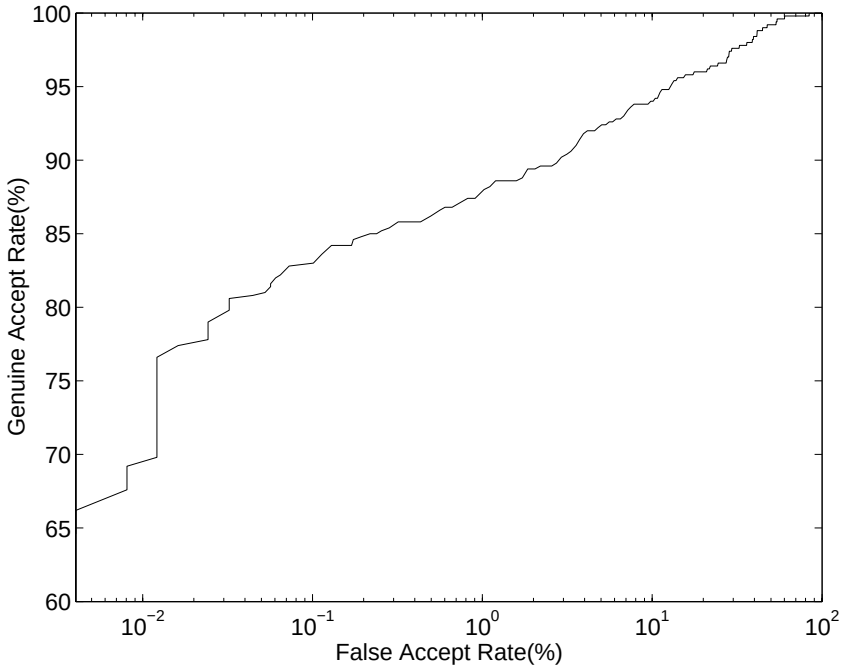


Figure 12. Receiver operating characteristics of the on-line signature recognition algorithm.

Acknowledgements

We would like to thank Umut Uludag for many helpful discussions and suggestions.

REFERENCES

1. B. Schneier, *Applied Cryptography*. John Wiley & Sons, 1996.
2. M. Wu and B. Liu, *Multimedia Data Hiding*. Springer, 2002.
3. F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding - a survey," *Proc. of the IEEE*, vol. 87, pp. 1062–1078, July 1999.
4. F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. of the IEEE*, vol. 87, pp. 1079–1107, July 1999.
5. A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, pp. 1494–1498, November 2003.
6. D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proc. of the IEEE*, vol. 87, pp. 1167–1180, July 1999.
7. M. M. Yeung and F. C. Mintzer, "Invisible watermarking for image verification," in *Proc. International Conference on Image Processing*, vol. 2, (Washington, DC), pp. 680–683, October 1997.
8. M. M. Yeung and S. Pankanti, "Verification watermarks on fingerprint recognition and retrieval," *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 468–476, 2000.
9. G. Voyatzis and I. Pitas, "Chaotic mixing of digital images and applications to watermarking," in *Proc. European Conference on Multimedia Applications*, vol. 2, pp. 687–695, May 1996.
10. A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, pp. 2963–2972, December 2002.
11. A. K. Jain, S. Pankanti, and R. Bolle (eds.), *BIOMETRICS: Personal Identification in Networked Society*. Kluwer, 1999.