A PRACTICAL PROTOCOL FOR DIGITAL AND PRINTED DOCUMENT AUTHENTICATION

Paulo Vinicius Koerich Borges[1], *Joceli Mayer*[2], *Ebroul Izquierdo*[1]

[1] Dept. of Electronic Engineering
Queen Mary University of London
Mile End Road, London E1 4NS, UK
Tel: +44 (0)20 7882-5346
vini@ieee.org, ebroul.izquierdo@elec.qmul.ac.uk

[2] Dept. of Electrical Engineering
Federal University of Santa Catarina
Trindade, 88.040-900, Florianpolis, Brazil
Tel: +55 48 3721-7627
mayer@eel.ufsc.br

ABSTRACT

This paper discusses a practical protocol for text document authentication, applicable to digital and printed form documents. It uses the text characters information to determine a key used to generate an authentication vector. Based on this vector, a feature in each character of the document is modified, without affecting the character "meaning." The modifiable feature may be size, color, shape, relative position, among others. If any character on the text is changed, the character information is different and consequently the authentication vector is also different. The proposed system does not require database retrieval and it is extremely difficult to forge the authentication process. A correlation-based detector for the system is proposed, and because feature detection errors may occur, an analysis is performed to determine the false alarm error probability of the system. Experiments illustrate the applicability of the method, considering the digital and the printed cases.

1. INTRODUCTION

Due to the undesired financial and security impact that fraudulent documents often cause, document authentication is seen as indispensable research area which has experienced significant growth in recent years.

Regarding paper form, traditional authentication methods include bar codes, holographic and plastic seals, physical paper watermarks, and authorized personnel handwritten signatures. However, modifications in the text can be carried out unnoticeably, changing the meaning of the document. Documents with bar-codes, for example, can be scanned, modified, and re-printed, and the bar-code will still be the same. Handwritten signatures can always be forged, and stamps counterfeited. Additionally, all these strategies cause a strong visible impact to the original document, which is an aspect often undesired.

This paper proposes a novel document authentication system which can be applied to electronic and printed documents, possibly to be used in conjunction with the traditional methods mentioned above. The system resembles the method proposed in [18], however the channel noise is considered in the detection process. The system can be set to cause a very low perceptual impact and unlike a digital signature, which protects the binary codes of the documents, the system proposed here protects the visual content. In contrast to the digital watermarking schemes [9] that transmit a hidden message, the proposed system classifies the document as authentic or non-authentic.

An advantage of the system is that it does not require a database to store information to be compared. For this reason, the proposed system is coined text self authentication (TSA). Moreover, special hardware is not required, except for a consumer scanner when printed documents are considered. Notice that TSA does not rely on a specific function to modify each character, which can be either performed with very low perceptual impact using text watermarking techniques [1, 2, 10], or visibly to increase robustness.

Two applications scenarios are considered. In the first scenario, TSA is described in a noise-free environment and the false alarm rate (ie., the probability of assigning an authentic document as non-authentic) is zero. In this case, the system resembles the method proposed in [18]. In the second scenario, however, it is assumed that errors may occur in the detection of the modified character feature, mainly due to the noise in print and scan (PS) process. In this case, a correlation-based detector is proposed and an analysis is performed to determine the detection error probability. Applications include passports, driver's licenses and ID cards, and legal notes.

This paper is organized as follows. Section 2 describes the proposed method and discusses related approaches. Section 3 performs an analysis to determine the false alarm probability due to the noise in the PS process. Section 4 presents experimental results, followed by conclusions in Section 5.

2. A PRACTICAL AUTHENTICATION PROTOCOL

As discussed in [1], a possible approach to text document authentication is to consider text as a data structure consisting of several modifiable features such as size, shape, position, luminance, color, halftone screen, etc. These features can be modified, possibly unperceptually to the human eye, according to a side message (or watermark message) to be embedded in the document. Examples of practical implementations proposed in the literature include text luminance modulation (TLM) [1, 2], color modulation [1], position (character shift coding, word shift coding, line shift coding) [10], size, and pixel toggling [11]. Other options are modifying the halftoning algorithm [1, 17] or even the printer mechanism [16].

Most of the above methods can be applied in the TSA protocol. However, for the system description and the examples in this paper, luminance is chosen as the modifiable feature. Therefore, TLM is used to allow easy visible illustration of the underlying process. An example of TLM is given in Fig. 1.

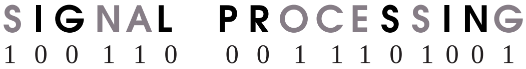


Figure 1: Example of text watermarking through luminance modulation.

The proposed framework for authentication scrambles the binary representation of the original text string with a key that depends on the string. The resulting scrambled vector is used to create another vector of dimension equal to the number of characters in the document. This is used as a rule to modulate each character individually. Fig. 1 illustrates the modulation process, where characters luminances are the modulated features.

Related approaches for image authentication in which a digital watermark is generated with a key that is a function of some feature f in the original image have been proposed in the literature, as in [5, 6, 12, 13], for example. To avoid that f be modified by the embedding of the watermark itself, hence frustrating the watermark detection process, only characteristics of a portion of the image must be used. It is possible, for example, to extract features from the low-frequency components, and to embed the watermark in the high frequency components, as discussed in [3].

In contrast, in the authentication system proposed here, the modified characters luminances do not alter the feature used to generated the permutation key, which are the characters "meanings." The system is described in the following.

2.1 Encryption

A block diagram of the encryption process is presented in Fig. 2.

- Let vector $\mathbf{c} = [c_1, c_2, \ldots, c_K]$ of size K represent a text string with K characters.
- Let vector $\mathbf{s} = [s_1, s_2, \ldots, s_K]$ represent the luminances of characters $[c_1, c_2, \ldots, c_K]$, respectively.
- Let $c_i \in \Omega$ ($\Omega = \{$a,b,c, …, X, Y, Z $\}$, for example), where Ω has cardinality S.
- Let c_{bi} be the binary representation of symbol c_i.
- Let $\mathbf{c}_b$ be the binary representation of $\mathbf{c}$, where $\mathbf{c}_b$ has size $|\mathbf{c}_b| = K \log_2 S$.
- Let $\kappa = f(\mathbf{c}_b)$ be a function of $\mathbf{c}_b$. κ is used as a key to generate a pseudo-random sequence (PRS) $\mathbf{k}$, such that the PRS's are ideally orthogonal for different keys κ.
- Let $\mathbf{c}'_b = \mathbf{c}_b \oplus \mathbf{k}$, where $\oplus$ represents the "exclusive or" (XOR) logical operation.
- Let $\mathscr{M}$ be a function that maps $\mathbf{c}'_b$, with $|\mathbf{c}_b|$ bits, to another vector $\mathbf{w}$, with K bits.

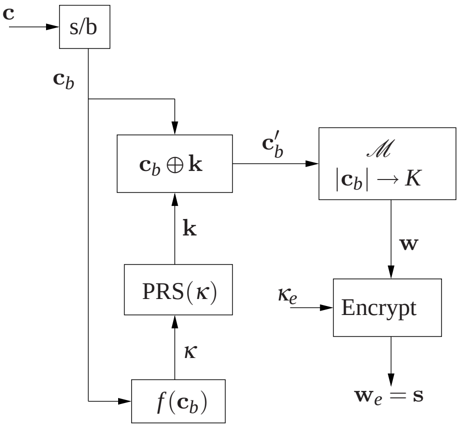


Figure 2: Encryption block diagram. Block 's/b' represents string-to-binary conversion. Block '$\mathscr{M}$' represents a mapping of $\mathbf{c}'_b$ from $|\mathbf{c}_b|$ bits to K bits. The symbol $\oplus$ represents the "exclusive or" (XOR) logical operation.

In order to provide security, $\mathbf{w}$ is encrypted with the private key of a public key cryptosystem [4]. Public key cryptosystems use two different keys, one for encryption, κ_e, and one for decryption, κ_d. The private key κ_e is only available for users who are allowed to perform the authentication process. On the other hand, anyone can have access to the public key κ_d to *only check* whether a document is authentic, without the ability to generate a new authenticated document.

Let $\mathbf{w}_e$ be the encrypted version of $\mathbf{w}$ based on the key κ_e, using a public key encryption scheme such as the RSA [4], for example. To authenticate the text document, vector $\mathbf{s}$ (which represents the luminances of the characters in the document) is modified such that $\mathbf{s} = \mathbf{w}_e$. Therefore, the document is authenticated by setting the luminance of each character c_i equal to s_i.

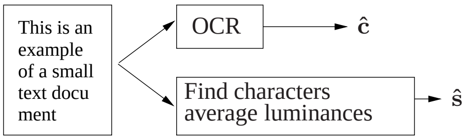

This is an example of a small text docu ment
OCR
$\hat{\mathbf{c}}$
Find characters average luminances
$\hat{\mathbf{s}}$

Figure 3: Extracting $\hat{\mathbf{c}}$ and $\hat{\mathbf{w}}$ from the received document.

2.2 Decryption

In the verification process, OCR is applied to the document in the printed cases. In addition, the average luminance of each character is determined, as illustrated in Fig. 3. Therefore, when testing for the authenticity of the document one has access to a received $\hat{\mathbf{c}}$ and a received $\hat{\mathbf{s}}$, where $\hat{\mathbf{c}}$ and $\hat{\mathbf{s}}$ represent the received vectors $\mathbf{c}$ and $\mathbf{s}$, respectively. It is assumed that the conditions are controlled such that no OCR or luminance detection errors occur. Moreover, one has access to a public key κ_d for decryption in the RSA algorithm and a permutation key $\kappa = f(\hat{\mathbf{c}}_b)$, which depends on $\hat{\mathbf{c}}$.

Using the public key κ_d, it is possible to decrypt $\hat{\mathbf{s}} = \hat{\mathbf{w}}_e$ into $\hat{\mathbf{w}}$. Using κ, it is possible to scramble $\hat{\mathbf{c}}_b$ (the binary representation of $\hat{\mathbf{c}}$) yielding $\hat{\mathbf{c}}'_b$. Applying the same mapping rule $\mathscr{M}$ of the encryption process to $\hat{\mathbf{c}}'_b$ yields a new vector $\hat{\mathbf{w}}'$.

If $\hat{\mathbf{w}}' = \hat{\mathbf{w}}$ the document is assumed authentic. Else, it is assumed that one or more characters have been altered. A block diagram of the authentication test process is given in Fig. 4.

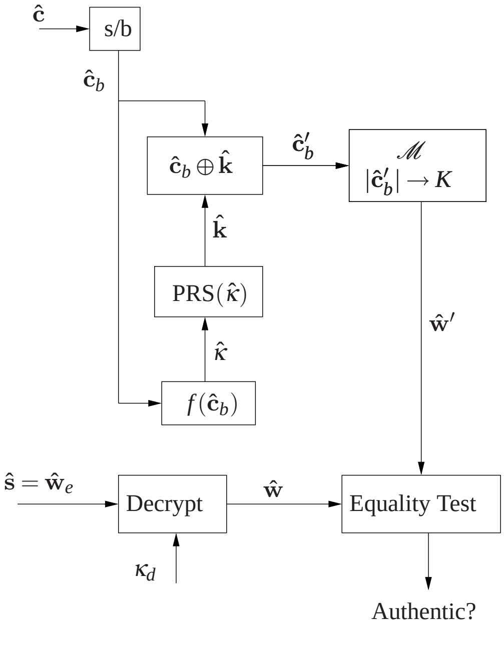


Figure 4: Decryption block diagram. Block 's/b' represents string-to-binary conversion. Block '$\mathscr{M}$' represents a mapping of $\hat{\mathbf{c}}'_b$ from $|\mathbf{c}_b|$ bits to K bits. The symbol $\oplus$ represents the "exclusive or" (XOR) logical operation.

If an attacker changes one or more characters in the document such that $\hat{\mathbf{c}} \neq \mathbf{c}$, $\hat{\mathbf{w}}$ and $\hat{\mathbf{w}}'$ are two completely different sequences (quasi-orthogonal) with very high probability, failing the authentication test.

Although in the above description OCR has been included in the detection process assuming that the document has been printed and scanned, the proposed authentication protocol can be applied to digital documents.

3. NOISY ENVIRONMENT

The final stage of TSA illustrated in Fig. 4 performs an equality test to decide whether a document is authentic. In noisy environments such as the PS channel, however, this approach can cause a high false alarm rate, that is, documents can be wrongly claimed as non-authentic. Therefore, a correlation test to determine the similarity between the expected $\hat{\mathbf{w}}$ and the received $\hat{\mathbf{w}}'$ is used. This is presented in Section 3.2, after a PS channel model is discussed in Section 3.1.

3.1 The Print and Scan Process

3.1.1 *The Halftoning Process*

This section describes the halftoning process, which occurs prior to printing. This description is focused on ordered dithering halftoning.

Let s be a digital image of size $M \times N$ with $L+1$ levels in the range [0,1], where **0 represents white** and **1 represents black**. A halftoned image (binary) b is generated from s, using the ordered dithering halftoning algorithm. The output of this method depends on the size and on the coefficients of the *dithering matrix D* of size $J \times J$, where each coefficient represents a threshold level and the coefficient values in D are approximately uniformly distributed. Each coefficient takes a value from the set $\{0, 1/L, 2/L, \ldots, 1\}$. The binary output image b is given by an element-by-element thresholding operation between the pixels in s and the coefficients in D. In general, $J \ll M$ and $J \ll N$. The input-output relationship of ordered dithering can be mathematically described by:

$$b(m,n) = \begin{cases} 0 & \text{if} \quad s(m,n) < D(m \bmod J, n \bmod J) \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

where the output '0' represents a white pixel (do not print a dot), and '1' represents a black pixel (print a dot). Clearly, the coefficients in D have a direct effect on the quality of the halftone image.

3.1.2 *Print and Scan Analytical Model*

Analytical models of the PS channel have been presented in the literature [7, 2]. In addition to the geometric distortions (possible rotation, re-scaling, and cropping), PS models assume that the process can be modeled by low-pass filtering, the addition of Gaussian noise, and non-linear gains, such as brightness and gamma alteration. In the following a PS channel model is described, which includes the halftone signal.

The digital scanned image y is represented by

$$\begin{aligned} y(m,n) = g_s\Big\{ & \big\{g_{pr}[b(m,n)] + \eta_1(m,n)\big\} * \\ & * h_{ps}(m,n)\Big\} + \eta_3(m,n), \end{aligned} \tag{2}$$

where b is the halftoned image generated from the original image s. η_1 represents printing noise due to microscopic ink and paper imperfections. The noise η_3 combines illumination and CCD electronic noise [7], as well as the quantization noise due to A/D. The operator $*$ represents convolution and the linear system h_{ps} is a low-pass filter combining the point-spread functions of the printer and of the scanner. In the printing process, blurring occurs due to toner or ink spread. In the scanning process, the low-pass effect is due to the optics and the motion blur caused by the interactions between adjacent CCD arrays elements [7].

The term $g_{pr}(\cdot)$ in (2) represents a gain in the printing process. In practice, when toner or black ink particles are applied over the paper, they do not present a null reflectance, causing a luminance gain to the printed image [15]. This distortion is described by $g_{pr}(m,n) = \alpha(m,n)b(m,n)$, where α is a gain affecting the black elements of b. α is modeled as constant for a small region (an area corresponding to a full character, for example), but it does vary throughout a full page due to non-constant printer toner distribution.

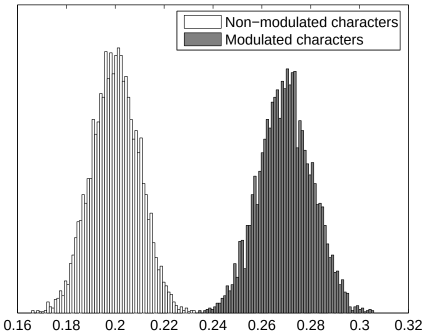


Figure 5: Distribution of the average luminance.

The term $g_s(\cdot)$ represents the response of scanners, which vary depending on the device. They may cause a non-linear gain to the scanned image, represented by $g_s(m,n) = [x(m,n)]^{\phi}$ as reported in results presented in [7].

In the model in (2), it is possible to decompose b into a constant term $\bar{b}$ added to a noise term η_2, such that $b(m,n) = \bar{b} + \eta_2(m,n)$. Therefore, assuming that b is generated from a constant gray level region (as in the TLM application), that is, $s(m,n) = s_0 = \bar{b}$, (2) can be written as

$$\begin{aligned} y(m,n) = g_s\Big\{ & \big\{g_{pr}[\bar{b} + \eta_2(m,n)] + \eta_1(m,n)\big\} * \\ & * h_{ps}(m,n)\Big\} + \eta_3(m,n), \end{aligned} \tag{3}$$

3.2 Detection

The simplest detection metric to determine embedded luminance is the average luminance of the element, given by (4). It is known from detection theory [14] that this detection statistic is the Neyman-Pearson detector (which minimizes the error probability) when detecting a change in the mean level considering Gaussian noise, which is the framework of the application.

By mapping the (m,n) coordinates to an one-dimensional notation, the detection metric w_i for the i-th character is given by:

$$w_i = \frac{1}{N_i} \sum_{n=1}^{N_i} y_i(n), \tag{4}$$

where N_i is the number of pixels in character i and $y_i(n)$ is the printed and scanned version of $s_i(n)$, according to the PS model described in (2).

Due to the nature of the noise and based on experimental observations, the noise terms η_1 and η_3 can be generally modeled as zero-mean independent Gaussian noise [7, 2]. Regarding the noise η_2, although it is zero-mean and may be assumed approximately uncorrelated, it is not normally distributed. However, considering the sum of the several distortions of the channel, it is observed experimentally that the detector output w can be modeled as normal random variable as supported by the Central Limit theorem [14]. This assumption is illustrated in Fig. 5, where the distribution of the average luminance of 10,320 printed and scanned characters is presented. This is also supported by experiments presented in [2]. A normal distribution can also be assumed for the result of the detection in line shift coding algorithms [8].

Hence, it is assumed that

$$\hat{\mathbf{w}} = \mathbf{w} + \mathbf{n}, \tag{5}$$

where $\mathbf{n}$ is modeled as additive white Gaussian noise (AWGN).

Therefore, instead of using an equality test, a correlation detector to check the similarity between the expected $\hat{\mathbf{w}}$ and the received $\hat{\mathbf{w}}'$ is used. In this case, the document is assumed authentic if the result of the linear correlation T between $\hat{\mathbf{w}}$ and $\hat{\mathbf{w}}'$ is greater than a given threshold λ. Linear correlation is employed as it is the optimal robustness metric when the channel can be modeled by AWGN [9].

Therefore, in the proposed correlation test the document is assumed authentic if

$$T = \frac{1}{K}\sum_{i=1}^{K} \hat{w}_i \hat{w}'_i > \lambda \tag{6}$$

where T is a normally distributed random variable and $\hat{w}_i$ and $\hat{w}'_i$, $i = 1,\ldots,K$ are the elements in $\hat{\mathbf{w}}$ and $\hat{\mathbf{w}}'$, respectively. When the document is authentic, vector $\hat{\mathbf{w}}'$ is given by $\hat{\mathbf{w}}' = \hat{\mathbf{w}} + \mathbf{n}$. When the document is tampered with, it is expected that

$$\hat{\mathbf{w}} \perp \hat{\mathbf{w}}' \therefore \frac{1}{K}\sum_{i=1}^{K} \hat{w}_i \hat{w}'_i = 0 \tag{7}$$

Assuming that $\mathbf{n}$ and $\hat{\mathbf{w}}$ are distributed according to $\mathbf{n} \sim \mathcal{N}(0,\sigma_n^2)$ and $\hat{\mathbf{w}} \sim \mathcal{N}(\mu_w,\sigma_w^2)$, the expected value in (6) is given by

$$\begin{aligned} \mu_T &= E\left\{\frac{1}{K}\sum_{i=1}^{K} \hat{w}_i(\hat{w}_i + n_i)\right\} = \frac{1}{K}\sum_{i=1}^{K} E\{\hat{w}_i^2\} + E\{\hat{w}_i n_i\} \\ &= \mu_w^2 + \sigma_w^2 \end{aligned} \tag{8}$$

The variance of (6) is given by

$$\sigma_T^2 = E\left\{\left(\frac{1}{K}\sum_{i=1}^{K} \hat{w}_i(\hat{w}_i + n_i)\right)^2\right\} - \mu_T^2 = \frac{(\mu_w^2 + \sigma_w^2)\sigma_n^2}{K} \tag{9}$$

The conditional error probability p_0 given that the document is tampered with is $p_0 = \Pr(T > \lambda|\text{tampered})$, where λ is a decision threshold. Defining the complementary error function $\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt$, $p_0 = \frac{1}{2}\operatorname{erfc}\left(\frac{\lambda - \mu_{T/0}}{\sqrt{2\sigma_{T/0}^2}}\right)$, where $\mu_{T/0}$ and $\sigma_{T/0}^2$ are respectively the mean and the variance of T for tampered with documents. Equivalently, if the document is authentic, the conditional error probability is given by $p_1 = \frac{1}{2}\operatorname{erfc}\left(\frac{\mu_{T/1} - \lambda}{\sqrt{2\sigma_{T/1}^2}}\right)$, where $\mu_{T/1}$ and $\sigma_{T/1}^2$ are respectively the mean and the variance of T for authentic documents. Finally, the average error probability is expressed by

$$P_{e_{d_M}} = P_0 p_0 + P_1 p_1 \tag{10}$$

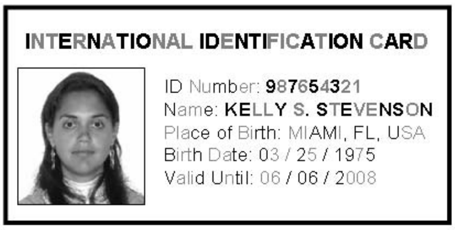
where P_1 and P_0 are the probabilities of occurrence of authentic and tampered with documents, respectively.

4. EXPERIMENTS

This section illustrates both printed and digital form applications for the proposed authentication method. It also presents a computer simulation to validate the analysis of Sec. 3.

4.1 ID Card

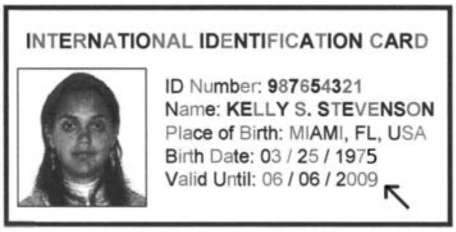
An identification card is authenticated through TSA, using TLM to modify the characters, as shown in Fig. 6. Notice that the intensity changes are visible to illustrate the underlying process. A modified version of the card is generated, where the last digit in the 'Valid Until' field is modified. To reduce the probability of OCR and luminance detection errors, only numbers and upper and lower cases characters of the alphabet are considered in this test.



INTERNATIONAL IDENTIFICATION CARD

ID Number: 987654321
Name: KELLY S. STEVENSON
Place of Birth: MIAMI, FL, USA
Birth Date: 03 / 25 / 1975
Valid Until: 06 / 06 / 2008

Figure 6: ID authenticated using TSA.



INTERNATIONAL IDENTIFICATION CARD

ID Number: 987654321
Name: KELLY S. STEVENSON
Place of Birth: MIAMI, FL, USA
Birth Date: 03 / 25 / 1975
Valid Until: 06 / 06 / 2009

Figure 7: Scanned ID. The last digit is modified from 8 to 9, as indicated by the arrow.

For the non-tampered document in Fig. 6, using a 8-bit ASCII table to represent the characters [4], the following parameters (discussed in Section 2) are obtained:

- $K = 124$, $\mathbf{c} = \{$I,N,T,E,R,N,$\ldots$,2,0,0,8$\}$.
- $\mathbf{c}_b = [0100100101001110,\ldots,00111000]$.
- $\kappa = f(\mathbf{c}_b) = 1176020$.
- $\mathbf{k} = [0100110110101110,\ldots,00010101]$.
- $\mathbf{c}'_b = \mathbf{c}_b \oplus \mathbf{k} = [0000010011100000,\ldots,00101101]$.
- $\mathbf{w} = [11100,\ldots,0110]$.
- $\mathbf{w}_e = [01101,\ldots,0111]$.

$\mathbf{w}_e$ is composed of K elements, corresponding to the number of characters in the document. The document is authenticated by altering the luminance of each character c_i in $\mathbf{c}$ to w_{ei} in $\mathbf{w}_e$. Notice that the characters luminances in the document in Fig. 6 are modified according to $\mathbf{w}_e$.

After printing, the parameters are obtained for two cases: one based on the authentic document and one based on the tampered with printed document in Fig. 7. For the authentic document, the document is correctly assigned as authentic. However, because the last digit of the tampered with document is different, $\hat{\mathbf{w}}$ and $\hat{\mathbf{w}}'$ are two completely different sequences, failing the test.

4.2 Paper Title

Some of the characters luminances on the title of this paper are slightly modulated to a gray level. This can be verified using any screen capture tool and common image processing software. Increasing the luminance gain to a visible level, the text becomes:

A PRACTIC AL PROTOCOL FOR DIGITAL AND PRINTED DOCUMENT AUTHENTICATION

Using the 8-bit ASCII standard, the parameters for this sample are:

- $K = 49$, $\mathbf{c} = \{$D,o,c,u,m,e,$\ldots$,i,o,n,s$\}$.
- $\mathbf{c}_b = [0100010001101111,\ldots,01110011]$.

which yields the modulation string $\mathbf{w}_e = [10011101,\ldots,1011]$ as illustrated in the characters luminance. If the 'D' in 'Document' is modified to 'd':

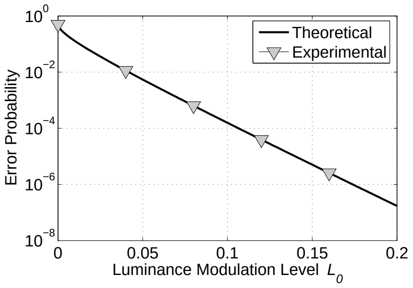


Figure 8: Detection error rates.

- $K = 49$.
- $\mathbf{c} = \{$d,o,c,u,m,e,$\ldots$,i,o,n,s$\}$.
- $\mathbf{c}_b = [110010001101111, \ldots, 01110011]$.

a completely different string $\mathbf{w}_e$ is generated:

$\mathbf{w}_e = [01100100, \ldots, 1000]$. and the authentication is not verified.

4.3 Error Rate

In this experiment, a text digital sample image g composed of 26 characters (as in 'abcd...z') is generated. Based on g, $800,000$ images g_j have their characters luminances randomly modulated according to a random $\mathbf{w}_j$, where $w_{ij} \in \{0, L_0\}$ with equal probability, $i = 1, \ldots, 26$ and $j = 1, \ldots, 800,000$. To simulated the effect of the PS channel over the average luminance of each character, noise term $\mathbf{n}_j$ is added to $\mathbf{w}_j$, as described in Section 3.

The correlation detector in (6) is applied to determine whether the document is authentic, based on the threshold λ. The error rates are shown in Fig. 8, according to the modulation energy L_0. The full line represents the theoretical error rate determined in (10). The triangles represent the error rate observed in the simulation, presenting an excellent correspondence to the theoretical curve. This illustrates that once the parameters of the PS system is determined, the performance of the authentication protocol can be predicted. In this experiment, the noise power is set to $\sigma_n^2 = 0.05$. Although Fig. 8 validates (10), real PS experiments have indicated that typical noise values are $\sigma_n^2 = 10^{-4}$. This causes the error rate to be virtually zero, illustrating the efficiency of the proposed method.

5. CONCLUSIONS

This paper describes a system that identifies frauds in text documents. The system does not require the use of appended files and it is robust to format conversions, such as PDF to Post Script, for example. Hence, unlike a digital signature, which protects the binary codes of the documents, the proposed system protects the visual content or the meaning of the document. Moreover, it can be set to be robust to the PS channel, providing perceptual transparency. Details on the algorithm are given in Section 2. To reduce detection errors due to the noise in the PS channel, a correlation detector is proposed. In this scenario, an analysis determines the detection error probability. Experiments validate the analysis and illustrate the applicability of the authentication method, using the title of this paper as one of the examples. Applications for the proposed system include authentication of passports, driver's licenses, and digital documents with sensitive content.

REFERENCES

[1] R. Vllan, S. Voloshynovskiy, O. Koval, J. Vila, E. Topak, F. Deguillaume, Y. Rytsar and T. Pun, "Text data-hiding for digital and printed documents: theoretical and practical considerations" in *Proc. of SPIE, Elect. Imaging,* USA, 2006.

[2] P. V. Borges and J. Mayer, "Document watermarking via character luminance modulation," *IEEE Int'l Conf. on Acoustics, Speech and Signal Processing,* May 2006.

[3] Ingemar J. Cox, Matthew L. Miller and Jeffrey A. Bloom, *Digital Watermarking,* Morgan Kaufmann, 2002.

[4] B.Sklar *Digital Communications* Prentice-Hall 2001.

[5] J. Cannons and P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," in *IEEE Trans. on Image Processing,* Vol. 13, Issue 10, Oct. 2004.

[6] X. Li and X. Xue, "Fragile authentication watermark combined with image feature and public key cryptography," in *7th Int'l Conf. on Signal Processing,* ICSP '04. 2004.

[7] N. D. Quintela and F. Prez-Gonzlez. "Visible encryption: Using paper as a secure channel." In *Proc. of SPIE,* USA, 2003.

[8] S. Low and N.F. Maxemchuk, "Capacity of text marking channel," in *IEEE Signal Proc. Letters,* Vol. 7, December 2000.

[9] Mauro Barni, Franco Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications,* Marcel Dekker, 2004.

[10] J.T. Brassil, S. Low, N.F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," *Proc. of IEEE,* Volume 87, No. 7, pp. 1181-1196, July 1999.

[11] Min Wu and Bede Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia,* Aug. 2004.

[12] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. on Image Processing,* Oct. 2001.

[13] V. Monga and B. L. Evans, "Robust perceptual image hashing using feature points Monga," *IEEE Int'l Confer. on Image Processing,* 2004. Volume 1, 24-27 Oct. 2004 Page(s):677 - 680 Vol. 1.

[14] S. M. Kay, Fundamentals of Statistical Signal Processing - Detection Theory, Prentice Hall, 1998.

[15] M. Mese and P.P. Vaidyanathan, Recent advances in digital halftoning and inverse halftoning methods, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* Vol. 49, Issue 6, June 2002 Page(s):790 - 805.

[16] Sungjoo Suh, Jan P. Allebach, George T.-C. Chiu, and Edward J. Delp,"Printer mechanism-level data hiding for halftone documents," *Proceedings of the IS&T's NIP22: International Conference on Digital Printing Technologies,* Denver, CO, September 17, 2006, pp. 436-440.

[17] Dhiraj Kacker and Jan P. Allebach, "Joint halftoning and watermarking," IEEE Transactions on Signal Processing, Volume 51, No. 4, April 2003 Page(s):1054-1068.

[18] R. Villan, S. Voloshynovskiy, O. Koval, F. Deguillaume and T. Pun, "Tamper-proofing of electronic and printed text documents via robust hashing and data-hiding," *in Proceedings of SPIE-IST Electronic Imaging 2007, Security, Steganography, and Watermarking of Multimedia Contents IX,* San Jose, USA, 2007.