JOINT AUTHENTICATION AND FORWARD ERROR CORRECTION OF STILL IMAGES

Alessandro Neri, Daniele Blasi, Patrizio Campisi, and Emanuele Maiorana

Department of Applied Electronics, Università degli Studi “Roma TRE”
Via della Vasca Navale 84, 00146, Roma, Italy
phone: + (39) 0657337017, fax: + (39) 0657337026, email: neri@uniroma3.it
web: www.comlab.uniroma3.it

ABSTRACT

Providing protection to the transmission of digital multimedia contents is nowadays an important requisite for many applications. However, it can also represent a great challenge, especially when dealing with wireless channels where, apart from preventing illegal data access, it would desiderable to possess the ability of discriminating between malicious data modifications and data distortions due to noise.

In this paper we present a joint authentication, integrity verification and channel coding scheme, applied to the secure image transmission scenario. Experimental results, obtained through Monte Carlo simulations, show that the employed security mechanisms guarantee an efficient and secure way for real-time image encryption and transmission through wireless networks.

1. INTRODUCTION

Multimedia contents are nowadays employed in many important and widely-spread applications, such as digital television, video conferencing, medical imaging systems, and so on. Digital media such as images offer the conveniences to be easily interpreted, synthesized, processed and edited, thus resulting in data which can be efficiently used to convey many kinds of information. However, on the other hand, they can also be easily copied by unauthorized subjects, or intentionally tampered by malicious attackers when transmitted. Therefore, emphasis should be given to such aspects when performing image transmission through wireless networks. Specifically, it is crucial to guarantee secure communication when data are transmitted through wireless channels.

Cryptographic techniques are usually employed to provide protection to sensitive information. Specifically, data encryption makes private information unintelligible to unauthorized users. Digital signatures can be employed to protect the confidentiality and the authenticity of the exchanged messages [1]. However, due to the noisy nature of a wireless channel or of the long term storage of multimedia documents, the presence of errors makes the use of encryption critical. For example, when considering encryption over a wireless transmission, the sensitivity to noise may result in the necessity of frequent data retransmissions, thus reducing the overall throughput. In order to improve the ciphers' performances in noisy environments, channel coding has to be therefore performed after encryption. Severe constraints in terms of Forward Error Correction (FEC) have to be specified in order to guarantee that the original messages can be properly deciphered and authenticated.

Error Correcting Codes (ECC) have been employed in [2] in conjunction with an embedded wavelet coding scheme to provide error resilience to images transmitted over wireless channels, while allowing to independently decode the different layers in which the information is partitioned. Therefore, the method in [2] is suitable to applications using block coding schemes, such as those defined by the JPEG2000 standard. A coding scheme able to provide encryption and error correction has been proposed in [3], where the trade-off between the throughput and the security achievable by means of ECCs has been analyzed. Turbo-codes [4] have been first considered in order to provide error-resilience for secure transmission over noisy channels in [5]. They have also been employed in [6] in conjunction with a genetic algorithm-based method, used to reduce the optimization complexity. Moreover, protection schemes based on turbo-codes, and specifically designed for secure image transmission over noisy channels, have been defined in [7], where the advanced encryption standard (AES) is employed to perform cryptographic encryption, and in [8], where the authors resort to 2-D chaotic logistic maps in order to reduce the computational complexity of the approach.

Although providing security and error resilience, such schemes do not take into account the authentication issues which should be considered when transmitting messages over wireless channels, where an attacker can tamper or substitute a legitimate message. For image or multimedia transmissions, such aspects are usually dealt with by means of watermarking approaches [9], which can also be employed to detect the performed tampering [10], or even to jointly perform image authentication and correction [11]. However, it should be noted that watermarking approaches necessarily alter the original contents, in order to embed a signature sequence.

In this paper, we propose a scheme which jointly provides encryption, authentication, and forward error correction for image transmissions over noisy channels, by means of turbo-codes with semi-random interleavers, selected among a wide collection, in accordance to a predefined session key. As already remarked in the authors' work in [12], and by recent studies on noisy channels [13], [14], a tight cooperation between channel coding and security mechanisms

© EURASIP, 2010 ISSN 2076-1465

should be exploited to reduce the security overhead, to decrease the requested computational complexity, and to achieve the secrecy capacity limit. The proposed approach, detailed in Section 2, guarantees a strong resilience to the errors introduced by noisy channels, while providing the means to discriminate between data modifications performed by malicious attackers, and data distortions due to noise. Moreover, data encryption, performed before channel coding to prevent illegal data access, is also exploited to improve the performances of the proposed scheme, in terms of lower bounds on the probability of impersonation, substitution, and deception, as pointed out by Simmons in [15].

The Monte Carlo simulations performed to test the proposed secure image transmission scheme are presented in Section 3, while some conclusions are drawn in Section 4.

2. PROPOSED SCHEME

The encoder employed to safely transmit an authenticated image over a noisy channel in presence of a malicious opponent, and the decoder employed to receive the image and determine if it is original, are respectively given in Figure 1 and Figure 2. The following subsections describe in details the characteristics of the proposed architectures.

2.1 Encoder

The proposed encoder consists of two-stages. In the first one, following the Shannon's substitution-permutation paradigm, the bitstream $\boldsymbol{m}$, representing the image, is divided into blocks of N bits, and each block is XORed with a pseudo-random binary i.i.d. sequence. The remaining statistical structure of the encrypted block is then dissipated by permuting it by means of a pseudo-random interleaver Π_C, thus obtaining the sequence $\boldsymbol{s}$. It is worth noting that the pseudo-random encryption sequence and interleaver are selected on the basis of the session key k_C, and that both the employed dictionaries should be constructed in order to allow the turbo-encoder to guarantee high correction rates.

The second stage is a parallel turbo-code, consisting of two interleavers Π_1 and Π_2, two recursive convolutional coders C_1 and C_2, and two puncturing blocks P_1 and P_2. Each element of the turbo-encoder is selected from a predefined dictionary, based on the output of a pseudo-random generator driven by the vectorial secret key $\mathbf{k_A} = \left[k_{\Pi_1},\ k_{\Pi_2},\ k_{C_1},\ k_{C_2},\ k_{P_1},\ k_{P_2} \right]$ where the couple $\left[k_{\Pi_1},\ k_{\Pi_2} \right]$ establishes the interleaving patterns, the couple $\left[k_{C_1},\ k_{C_2} \right]$ the RSC (Recursive Systematic Convolutional) codes generator polynomials and finally $\left[k_{P_1},\ k_{P_2} \right]$ the position of the redundancy bits to be erased for the puncturing process. The pair (k_C, $\mathbf{k_A}$) represents the session key, and has to be periodically updated to properly guarantee communication security. The input to the modulator is therefore constituted by the ciphertext $\boldsymbol{s}$, which represents the systematic contribution of the turbo-encoder, and the punctured parity sequences z_1 and z_2, for a total of M bits. The turbo-code rate is given by the ratio $R = N/M$.

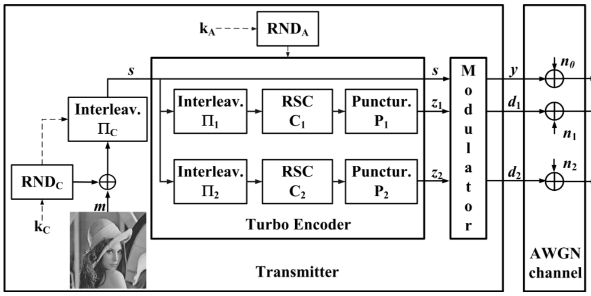


Figure 1 - Encoder scheme

When using an Additive White Gaussian Noise (AWGN) channel the received signal is given by:

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{y}+\boldsymbol{n}_0 = \mu(\boldsymbol{s})+\boldsymbol{n}_0, \\ \boldsymbol{r}_1 &= \boldsymbol{d}_1+\boldsymbol{n}_1 = \mu(z_1)+\boldsymbol{n}_1, \\ \boldsymbol{r}_2 &= \boldsymbol{d}_2+\boldsymbol{n}_2 = \mu(z_2)+\boldsymbol{n}_2, \end{aligned} \tag{1}$$

having denoted with $\mu(\cdot)$ the mapping from the binary input to the constellation points of the employed modulation, and where $\boldsymbol{n}_0 = \boldsymbol{n}_0^I + \boldsymbol{n}_0^Q$, $\boldsymbol{n}_1 = \boldsymbol{n}_1^I + \boldsymbol{n}_1^Q$, and $\boldsymbol{n}_2 = \boldsymbol{n}_2^I + \boldsymbol{n}_2^Q$ are Circularly Complex White Gaussian Noise samples, modelling the complex envelop of the receiver noise, whose in phase and in quadrature components are respectively denoted by the indexes I and Q.

2.2 Decoder and Authentication Procedure

The decoder and authentication schemes are depicted in Figure 2. The turbo-decoder produces the estimate $\hat{\mathbf{s}}$ of the original message, which is then used to test the authenticity of the received signal, together with the estimates $\hat{z}_1$ and $\hat{z}_2$ of the parity sequences. Specifically, let us indicate with H_0 the hypothesis that the message has been altered or forged, and with H_1 the hypothesis that the received signal is the noisy version of the authentic original message. Following a Bayesian approach, a decision about the integrity and authenticity of the received data can be performed by analyzing the ratio between the *a posteriori* probabilities of the two hypotheses, namely,

$$\frac{\Pr\{\hat{s}|\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2\}}{\sum_{\mathbf{s}_i \in F} \Pr\{\boldsymbol{s}_i|\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2\}}, \tag{2}$$

where $\mathscr{F}$ is the set of all forged/altered messages. However, such procedure results to be unfeasible, for both theoretical and practical reasons. From a theoretical point of view, the computation of (2) would require the knowledge of the *a priori* probability distribution of the attacks, which is usually unavailable. From a practical point of view, the computational burden of (2) prevents its evaluation even in the unrealistic case where the *a priori* probabilities of being attacked are known. Therefore, we resort to the adoption of the Neyman-Pearson procedure [16] in order to decide about authenticity and integrity of the received data.

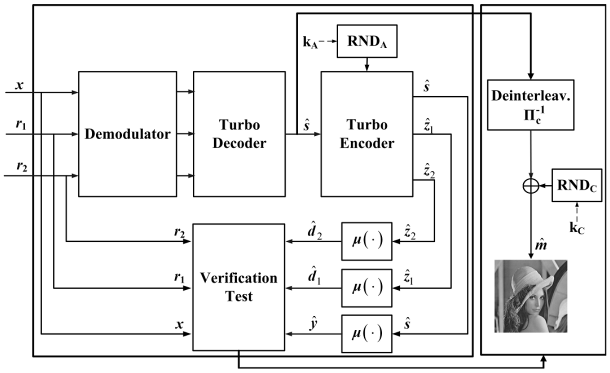


Figure 2 - Decoder scheme

In general, the user encodes the encrypted version of the image using a key $\mathbf{k_B}$. Once the M samples $[\boldsymbol{x}, \boldsymbol{r}_1, \boldsymbol{r}_2]$ are received they are turbo-decoded (using the correct key $\mathbf{k_A}$) into the N bits $\hat{s}$. At this point such bits are re-encoded using the key $\mathbf{k_A}$ into the M bits $[\hat{s},\ \hat{z}_1,\ \hat{z}_2]$. Since we refer to a Binary Phase Shift Keying (BPSK) modulation scheme, the last M bits are mapped into the M samples $[\hat{\boldsymbol{y}},\ \hat{\boldsymbol{d}}_1,\ \hat{\boldsymbol{d}}_2]$. It is clear that if $\mathbf{k_B} = \mathbf{k_A}$ or, in other words, the user is authentic, the difference between the M samples $[\boldsymbol{x}, \boldsymbol{r}_1, \boldsymbol{r}_2]$ and $[\hat{\boldsymbol{y}},\ \hat{\boldsymbol{d}}_1,\ \hat{\boldsymbol{d}}_2]$ will only be due to the noise. This case is what we denoted by H_1 and it is clear that the more this difference is greater, the less will be the log-likelihood $\log\Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2)$ of the decoded cipher-text, given the received signal, that is employed as the score of the authentication phase. A threshold λ, that represents the minimum value to for $\log\Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2)$ in order to decide to be in the H_1 case (e.g. the user is authentic). For these reasons, the decision rule should be:

$$\log\Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2) \underset{H_0}{\overset{H_1}{\gtrless}} \lambda. \tag{3}$$

In accordance to the Neyman-Pearson lemma, the threshold λ is selected in dependence on the maximum acceptable probability P_{fa} of false alarm, which is defined as the event of rejecting an authentic message. Obviously, such value is application dependent, and is intended to be as a system requirement. Having set the threshold to meet the false alarm probability requirements, we may choose the remaining parameters (e.g. turbo code rate, transmitting power, etc.), in order to maximize the probability of detecting any security attack.

A trade-off to meet additional constraints on maximum transmitting power, bit rate, hardware and software complexity, and so on, may be therefore required. As for the expression of the log-likelihood $\log\Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2)$, for AWGN channels it can be demonstrated that:

$$\log\Lambda(\hat{s};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2) = \log\Pr\{\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2/\hat{s}\} = -\frac{M}{2}\log 2\pi\sigma^2$$
$$-\frac{1}{2\sigma^2}[\boldsymbol{x}-\mu(\hat{s})]^{\dagger}[\boldsymbol{x}-\mu(\hat{s})] - \frac{1}{2\sigma^2}[\boldsymbol{r}_1-\mu(\hat{z}_1)]^{\dagger}[\boldsymbol{r}_1-\mu(\hat{z}_1)]$$
$$-\frac{1}{2\sigma^2}[\boldsymbol{r}_2-\mu(\hat{z}_2)]^{\dagger}[\boldsymbol{r}_2-\mu(\hat{z}_2)], \tag{4}$$

where † denotes the Hermitian operator, σ^2 is the receiver noise variance, and M is the sum of the sizes of the complex vectors $\boldsymbol{x}$, $\boldsymbol{r}_1$, and $\boldsymbol{r}_2$. When the bit error rate at the output of the decoder is small, which implies that $\hat{\boldsymbol{s}} \cong \boldsymbol{s}$, the log-likelihood functional $\log\Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2)$ can be well approximated, under the hypothesis H_1, as:

$$\log\Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2/H_1) \cong -\frac{\mathrm{M}}{2}\log 2\pi\sigma^2 - \frac{\nu}{2}, \tag{5}$$

being

$$\nu = \frac{1}{\sigma^2}\sum_{\mathrm{k}=0}^{2}\left(\left\|\boldsymbol{n}_{\mathrm{k}}^{\mathrm{I}}\right\|^2 + \left\|\boldsymbol{n}_{\mathrm{k}}^{\mathrm{Q}}\right\|^2\right) \tag{6}$$

a random variate with a chi-square distribution, with $2M$ degrees of freedom. Therefore, for the false alarm probability we obtain:

$$P_{fa} = \int_{-2\lambda - M\log 2\pi\sigma^2}^{\infty} p_{\chi^2_{2M}}(t)\,dt = \frac{\gamma\left(M,-\lambda-M\log 2\pi\sigma^2\right)}{(M-1)!} \tag{7}$$

where $\gamma(k,p)$ is the upper incomplete Gamma function:

$$\gamma(k,p) = \int_p^{\infty} t^{k-1}e^{-t}\,dt. \tag{8}$$

Thus, the authenticity threshold λ can be computed by numerical inversion of eq. (7), once P_{fa} is set. Threshold adaptivity requires the on-line estimation of the noise power spectrum density.

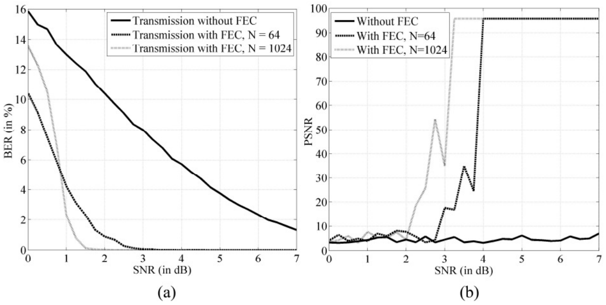
2.3 Authentication Performances

It is possible to analyze the performances of the proposed scheme with respect to the probability of impersonation, substitution and deception, as defined by Simmons [15]. Specifically, it can be demonstrated that the lower bound on the probability of impersonation P_I can be expressed in terms of the cardinality |ε| of the set of different systematic turbo-codes able to pass the authenticity and integrity tests:

$$P_I \geq \frac{1}{|\varepsilon|}. \tag{9}$$

The use of the pseudo-random interleaver Π_C is therefore useful also to improve the system authentication performances, by leveraging on the value of |ε|. We can also note that, as expected, the probability of impersonation attack increases in presence of noise, when |ε| decreases thus resulting in a higher bound, which is given by its inverse. It is also possible to demonstrate that the proposed architecture is unconditionally secure with respect to targeted substitution attacks, while presents a lower bound for the probability of deception P_D which can be expressed as

$$P_D \geq \frac{1}{\sqrt{|\varepsilon|}}. \tag{10}$$



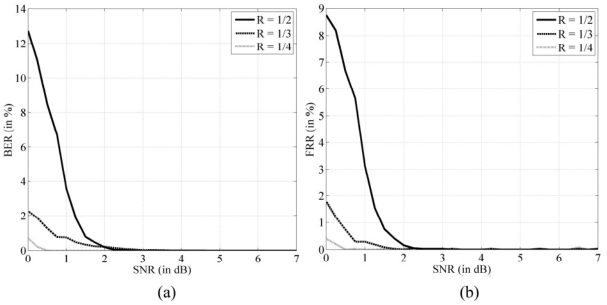
(a) (b)

Figure 3 - System performances when varying *N*, while keeping *R* = 1/2. (a): BER *vs*. SNR; (b): PSNR *vs*. SNR.

If the user is authentic, even in the case when some errors survive to the turbo-decoding the (eventual) burst error will be spread over the image bit-stream thanks to the kC-deinterleaving step. In this way the loss of integrity should not imply a sensible loss of quality.

3. EXPERIMENTAL RESULTS

The effectiveness of the proposed scheme for secure image transmission has been verified through an extensive set of Monte Carlo simulations. A single-carrier BPSK modulation has been used to simulate the transmissions of the images. We have first analyzed the system performances when varying the size *N* of the blocks at the input of the turbo-encoders, while keeping fixed the code rate *R* = 1/2. Figure 3(a) shows the achievable Bit Error Rate (BER) for different Signal-to-Noise (SNR) ratios, while Figure 3(b) reports the corresponding Peak Signal-to-Noise Ratio (PSNR) obtained for the received images. As can be seen, increasing the size of the input blocks results in improving the system's performances. It can also be seen that FEC has to be necessarily provided in order to deliver images with acceptable PSNR. We have also investigated the dependence of the system performances on the rate *R* employed for the turbo-codes: Figure 4(a) illustrates the BER achievable when keeping *N* = 256, while varying the code rate *R*, together with the code redundancy. We respectively denote by R_{c_1}, R_{c_2} and R_{p_1}, R_{p_2} the RSC codes and the puncturing rates of the scheme depicted in Figure 2, while $\boldsymbol{g_i} = [\boldsymbol{g_{\mathrm{FF}_i}}, g_{\mathrm{FB}_i}]$ is the vector of generator polynomial of the RSC code on the *i*-th encoding branch, being $\boldsymbol{g_{\mathrm{FF}_i}}$ the vector of feed-forward polynomials and g_{FB_i} the feed-back one. When the turbo-code rate *R* = 1/2: R_{c_1}=R_{c_2}=1/2, R_{p_1}= R_{p_2}=1/2, while (using octal notation) $\boldsymbol{g_{\mathrm{FF}_1}}$= $\boldsymbol{g_{\mathrm{FF}_2}}$=37 and g_{FB_1}= g_{FB_2}=21. When the rate *R*=1/3: R_{c_1}=R_{c_2}=1/3, R_{p_1}=R_{p_2}=1/2, while $\boldsymbol{g_{\mathrm{FF}_1}}$ = $\boldsymbol{g_{\mathrm{FF}_2}}$ = [37, 21] and g_{FB_1} = g_{FB_2} = 37. When *R* = 1/4: R_{c_1}=R_{c_2}=1/4, R_{p_1}=R_{p_2}=1/2, $\boldsymbol{g_{\mathrm{FF}_1}}$ = $\boldsymbol{g_{\mathrm{FF}_2}}$ = [37, 21, 37] and g_{FB_1} = g_{FB_2} = 21. Figure 4(b) reports the associated probability of rejecting an authentic message, also referred as False Rejection Rate (FRR). The reported curves have been computed with a probability of false alarm P_{fa}=10^{-5}. The increase of the code redundancy improves the BER performances, and it also results in an improvement of the FRR. Figure 5 shows the distributions of the scores to be used in the authentication phase.



(a) (b)

Figure 4 - Authentication performances when varying *R*, while keeping *N* = 256. (a): BER *vs*. SNR; (b): FRR *vs*. SNR.

Specifically, Figure 5(a) reports the normalized histogram of the samples of the random variate ν in (5) and (6), for a system where *N* = 10, *R* =1/2, P_{fa}=10^{-5}, and SNR=0 dB. More precisely, it can be noticed that the obtained histogram well fits with a chi-square distribution, which has been employed to derive the expression reported in Section 2.2. Figure 5(b) shows the distribution of the authentication scores $\log \Lambda(\hat{\boldsymbol{s}};\boldsymbol{x},\boldsymbol{r}_1,\boldsymbol{r}_2)$ in (5), and highlights where the threshold is automatically set by the employed procedure. It is worth reporting that the considered distributions vary when the SNR of the communication channel changes. Specifically, the random variate ν exhibits a distribution which can be very well approximated with a chi-square for SNR values lower than 5 dB, e.g., in practical channel conditions. It should also be noted that the range of the ν distribution is rather stable with respect to the channel SNR, while the distribution of the authentication scores in (5) is strongly affected by the observed SNR, and the same applies to the threshold λ, which is automatically evaluated by the proposed approach. The reported behaviours can be verified by comparing the histograms reported in Figure 5, obtained for SNR = 0 dB, with the ones shown in Figure 6, evaluated for SNR = 5 dB. Eventually, we have also analyzed the influence of the selection of the parameters *N* and *R*, which define the characteristics of the employed turbo-codes, on the cardinality |ε| of the set of different systematic turbo-codes which can be used to securely transmit images. As described in Section 2.3, the number |ε| of usable turbo-codes is directly connected with the probability of impersonation P_I and the probability of deception P_D: the lower the cardinality of the set of usable codes, the higher the probability of impersonation and deception. Figure 7 shows how the number of employable codes varies with *N* and *R*. It can be easily noticed that the cardinality |ε| always assumes high values, and that it also increases with the length N of the turbo-codes interleaver and with the rate *R*=*N*/*M*. The obtained values of |ε| guarantee very low probabilities of impersonation and deception, thus showing that the proposed scheme is robust with respect to these scenarios.

4. CONCLUSIONS

In the present paper we have dealt with the problem of providing a secure transmission mechanism for multimedia contents such as images, by presenting a joint authentication, integrity verification and channel coding scheme.

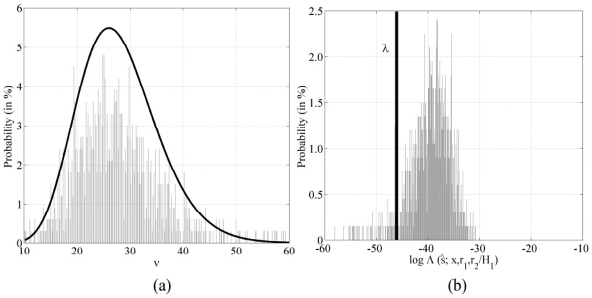


Figure 5 - Distributions of the authentication scores for SNR = 0 dB. (a): histogram of the ν samples with the chi-square estimated distribution; (b): histogram of the total authentication scores with the automatically estimated threshold.

The proposed approach can be employed for multiple scenarios like secure transmission of images over noisy channels where malicious attackers can try to tamper the data, as well as to provide protection and authentication for applications requiring long-term data storage, where the supports' degradation over time can alter the considered content by introducing errors in the carried data. Several experimental results have demonstrated the effectiveness of the proposed approach, able to discriminate between illegal data modification and data distortion due to noise, while preventing illegal data access by unauthorized subjects.

REFERENCES

[1] R.A. Mollin, *An introduction to cryptography*, Chapman and Hall/CRC, 2007.

[2] N.V. Boulgouris, N. Thomos, M.G. Strintzis, "Transmission of images over noisy channels using error-resilient wavelet coding and forward error correction", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 12, pp. 1170 - 1181, Dec 2003.

[3] C. Nanjunda, M.A. Haleem, R. Chandramouli, "Robust encryption for secure image transmission over wireless channels", in *IEEE ICC 2005*, 16-20 May 2005.

[4] C. Berrou, A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo-Codes", *IEEE Transaction on Communications*, Vol. 44, No. 10, pp. 1261–71, Oct. 1996.

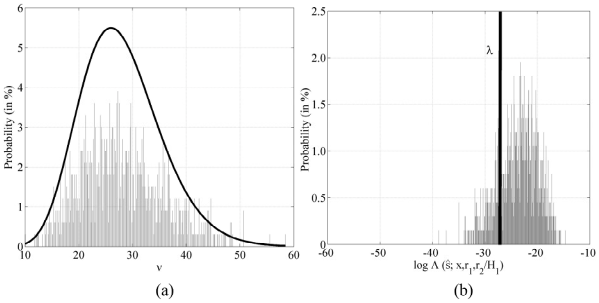


Figure 6 - Distributions of the authentication scores for SNR = 5 dB. (a): histogram of the ν samples with the chi-square estimated distribution; (b): histogram of the total authentication scores with the automatically estimated threshold.

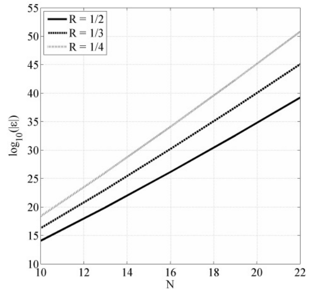


Figure 7 - Cardinality |ε| of the set of employable turbo-codes, varying the rate *R* and the interleaver length *N*.

[5] M. Padmaja, S. Shameem, "Secure Image Transmission over Wireless Channels", in *Int. Conf. on Computational Intelligence and Multimedia Apps. 2007*, 13-15 Dec. 2007.

[6] L. Yao. L. Cao, "Turbo Codes-Based Image Transmission for Channels With Multiple Types of Distortion", *IEEE Transactions on Image Processing*, Vol. 17, No. 11, pp. 2112 - 2121, Nov. 2008.

[7] H. Cam, V. Ozduran, and O. Ucan, "A combined encryption and error correction scheme: AES-Turbo", *Journal of electrical & electronics engineering*, Vol.1, pp. 861-866, 2009.

[8] M.A. El-lskandarani, S. Darwish, S.M.A. Abuguba, "A robust and secure scheme for image transmission over wireless channels", in *IEEE International Carnahan Conference on Security Technology (ICCST) 2008*, 13-16 Oct. 2008.

[9] C. Li, H. Song, "A novel watermarking scheme for image authentication in DWT domain", in *International Conference on Anti-counterfeiting, Security, and Identification in Communication (ASID) 2009*, 20-22 Aug. 2009.

[10] Y. Wa, "Detecting tampered image blocks using error correcting code", in *IEEE International Conference on Multimedia and Expo 2004*, 27-30 June 2004.

[11] J. Lee; C.S. Won, "A watermarking sequence using parities of error control coding for image authentication and correction", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 2, pp. 313–317, May 2000.

[12] A. Neri, D. Blasi, L. Gizzi, and P. Campisi, "Joint Security And Channel Coding For Ofdm Communications", in *EUSIPCO 2008*, Lausanne, Switzerland, August 25-29, 2008.

[13] L. Yingbin, H.V. Poor, S. Shamai, "Secure Communication Over Fading Channels", *IEEE Transactions on Information Theory*, Vol. 54, No. 6, pp. 2470-2492, June 2008.

[14] L. Lai; H. El Gamal, H.V. Poor, "Authentication Over Noisy Channels", *IEEE Transactions on Information Theory,* Vol. 55, No. 2, pp. 906-916, Feb. 2009.

[15] G.J. Simmons, "A survey of information authentication", *Proceedings of the IEEE*, Vol. 76, No. 5, pp. 603-620, May 1988.

[16] U.M. Maurer, "Authentication theory and hypothesis testing", *IEEE Transactions on Information Theory*, Vol. 46, No. 4, pp. 1350 – 1356, July 2000.