Information-Theoretic Data-Hiding for Public Network Security, Services Control and Secure Communications

Sviatoslav Voloshynovskiy[1], Frédéric Deguillaume[1], Oleksiy Koval[1] and Thierry Pun[1]

(Invited Paper)

headings

Abstract— **In this paper we introduce and develop a framework for the data-hiding technologies that aim at resolving emerging problems of modern public networks. First, we emphasize the main open issues in public network security, quality of services control and secure communications. Secondly, we formulate digital data hiding as communications with side information and advocate an appropriate information-theoretic framework for the analysis of different data hiding methods in various applications. In particular, Gel'fand-Pinsker channel coding with side information at the encoder and Wyner-Ziv source coding with side information at the decoder are used for this purpose. Finally, we demonstrate the possible extensions of this theory for watermark-assisted multimedia processing and indicate its perspectives for distributed networks.**

Keywords— **network security, telecommunications, copyright protection, tamper proofing, secure communications, robust watermarking, steganography.**

I. Introduction

The mass diffusion of digital media and the explosive growth of telecommunication are reshaping the lifestyles of ordinary people, research and industry. Over the last decade, the rise of digital telecommunication technologies (including ATM, PSTN, ISDN, ADSL, IP networks) has fundamentally altered how people work, think, communicate, and socialize. New emerging audio/visual applications have recently appeared thanks to the public multimedia networks. This growth is especially observed in networked video applications such as video phones, video conferencing, video e-mail, video streaming, digital TV, high-definition TV (HDTV), video on demand (VoD), distance learning, remote collaboration and surveillance.

However, despite the obvious progress of public networks, these developments carry with them a number of risks such as copyright violation, prohibited usage and distribution of digital media, secret communications, and network security. Therefore, security, scalability and manageability amongst others become issues of serious concern, as current solutions do not satisfy anymore the growing demands of multimedia communications.

In the scope of this paper, we will focus on a possible solution for public network security in order to prevent unauthorized data exchange and to ensure secure communications.

[1]The authors are with CUI-University of Geneva, Stochastic Image Processing Group, 24 rue General-Dufour, 1211 Geneva, Switzerland. The contact author is S. Voloshynovskiy (email: svolos@cui.unige.ch), http://sip.unige.ch

The paper has two main objectives. The first objective is to introduce and to overview a novel approach to multimedia security in public networks that is based on data-hiding technologies. We will consider fundamentals of digital data hiding technologies in comparison with the traditional means of multimedia security. A basic theoretical model of a data hiding system will be analyzed, and we will demonstrate the relevance of data hiding problems to digital communications. We will show the advantages of data-hiding based multimedia security protocols over the traditional general means of security based on encryption, scrambling and Firewall systems.

The second objective of the paper is to demonstrate some of the main achievements in the field of digital data-hiding technologies for multimedia network security and quality-of-service control. We will present the state-of-the-art solutions for copyright protection of digital media, integrity verification, detection of modifications of the multimedia content, and secure communications.

The paper is organized as follows: Section II outlines the main open issues in public networks. Sections III and IV introduce an alternative approach to public network security and secure communications based on digital data hiding and present the main problems to be addressed. Section V is dedicated to robust watermarking. Section VI considers integrity control and tamper proofing as well as watermark-assisted communications, and Section VII presents secure communications. Section VIII concludes the paper.

Notation. We use capital letters to denote scalar random variables X, bold capital letters to denote vector random variables $\mathbf{X}$, corresponding small letters x and $\mathbf{x}$ to denote the realizations of scalar and vector random variables, respectively. The superscript N is used to denote length-N vectors $\mathbf{x} = x^N = \{x[1], x[2], ..., x[N]\}$ with ith element $x[i]$. We use $X \sim p_X(x)$ or simply $X \sim p(x)$ to indicate that a random variable X is distributed according to $p_X(x)$. The mathematical expectation of a random variable $X \sim p_X(x)$ is denoted by $E_{p_X}[X]$ or simply by $E[X]$ and $\mathbf{Var}[X]$ denotes the variance of X. Calligraphic fonts $\mathcal{X}$ denote sets $X \in \mathcal{X}$ and $|\mathcal{X}|$ denotes a cardinality of set.

II. Open issues of public networks

An extremely rapid development of telecommunications has been observed in the last decades. First of all, it concerns general public networks such as asynchronous transfer mode

(ATM), public switched telephone networks (PSTN), integrated service digital network (ISDN), asynchronous digital subscriber line (ADSL) and cable and Internet protocol (IP) service. In the recent years, the explosion of audio/visual communications has caused additional interest towards multimedia applications of public networks, that are characterized by a huge amount of data to be stored or communicated preferably in real time. The data storage become extremely distributed, which leads to a number of problems related to reliable and secure data transportation, distributed computation and data management in distributed environments. Therefore, some questions of traditional communications should be reconsidered to satisfy new growing requirements. An ideal multimedia network is supposed to be capable of transferring reliably and securely any amount of information without delay and loss. Unfortunately, fundamental practical limitations and outdated main design principles of current networks do not meet these demands. With respect to that, security and quality-of-services are the main issues of concern (but not the only ones).

A. Network quality-of-service control

Practical public networks have a number of open issues related to quality-of-service (QoS) control. In practice, most of public networks cannot guarantee quality-of-service control due to many technical reasons, the main ones being[1]:

- Network errors (bit errors), loss and deletions (packet or bit loss), and insertions (cross talks). Data can be lost in the network for a variety of reasons, including congestion, rejection due to excessive delay, and network fault. These problems can manifest themselves as unnatural artifacts in the video and images, such as missing frames, lines, or blocks. Severe loss, such as from heavy network congestion, can cause the video playback to be stopped until the receiver can resynchronize. Moreover, errors arising from lost data can affect multiple video frames by temporal error propagation.
- Delay (real time), jitter (timing errors) and latency. Streaming multimedia is subject to delay constraints since the video must be decoded and displayed/played in real-time. If the video data spends too much time in the network, it is useless even if it arrives at the receiver. Buffering can reduce the effect of delay and jitter (timing errors). Latency can also be an issue when two-way communication is necessary.
- Finite bandwidth (network sharing, limited resources). Bandwidth is the amount of data that can traverse the network or a part of the network at any given time. Network bandwidth is a shared, limited resource and will vary with time. A network may not be able to guarantee that the required bandwidth for transporting multimedia data will be available.

In addition heterogeneity and time-variance are important factors for public network multimedia communications. A heterogeneous network is a network whose parts (sub-networks) may have vastly unequal resources. For example, some parts of a heterogeneous network may have abundant bandwidth and excellent congestion control while other parts of the network are overloaded and congested by overuse or by a lack of physical network resources. Different receivers on a heterogeneous network can experience different performance characteristics. When streaming video over a heterogeneous network, the video stream should be decodable at optimal quality for users with a good network connection, and at usable quality for users with a poor connection. Time-variance implies that bandwidth, delay, loss, or other network characteristics can significantly vary over time, sometimes drastically changing in a matter of seconds. The Internet is a difficult network for transporting real-time multimedia data, and is an example of a heterogeneous, time-varying, network with no QoS control.

B. Network security

Network security is no less important a problem of public networks. Due to the open nature of data communication protocols in public networks, special care about access control, authentication, secure delivery and intrusion detection should be taken. Traditional means of network security such as Firewalls, virtual private networks (VPN) and intrusion detection systems (IDS) are well suited for specialized applications where the above questions can be under control in the range of some closed trusted environment. However, these solutions are not appropriate for highly distributed public environments. Moreover, the definition of traffic *disregards the nature of the multimedia content*, interpreting any kind of multimedia as purely digital flow. This has a huge impact on many aspects of network security since modern secret communication tools based on steganalysis, viruses based on content embedding and content management systems are designed using completely different interpretation of the multimedia content. Moreover, contrarily to the traditional approaches, new public distributed networks cannot anymore rely on file headers, reliable meta data or centralized bodies. Recent examples of distributed networks based on P2P communications practically demonstrate how easily huge amount of information can be exchange in completely uncontrolled manner leading to secret communications, copyright violation and illegal or prohibited content distribution [2]. Traditional network security can hardly cope with these requirements.

Internet as a public network is a very challenging environment for secure and reliable transport of real-time multimedia data. Internet is a heterogeneous and time-varying network, has no QoS control and no efficient and reliable mechanisms for copyright protection, access control and secure communications. Therefore, we will below consider potential approaches that make at least partially possible to satisfy (or to complement existing solutions to) the above emerging problems.

III. Multimedia security: main open issues

Multimedia content security has a number of specific requirements that should allow to answer to the following questions:

- Who has issued the multimedia content?
- Who is the content owner?
- When was the content issued?
- Who has access right to the content?

- Is the content modified?
- Where was the content modified?
- What was the original content before modification?

It is obvious that specialized protocols or hardware alone are not able to resolve all these questions. At the same time, new emerging requirements to secure Internet communications essentially extended the horizons of traditional cryptography protocols. A new paradigm has to answer not only the question of how to communicate in a secure way but also how to communicate in a completely undetectable way over public networks. This subsequently leads to the extension of the concept of covert communications and requires the creation of new "covert" multimedia channels. Finally, the related open problem of quality-of-service control requires to provide the answer on the question how to communicate in a robust way providing end-to-end services?

The list of these diverse problems seems to be very broad and from a traditional point of view there does not seem to exist any common means of satisfying all these requirements. However, there are some common aspects of secure and reliable communications that could be addressed by novel technologies based on digital data hiding.

IV. Multimedia data-hiding

Multimedia data-hiding represents an alternative concept for public network security and secure communications and can be considered as an assisting functionality. Multimedia data-hiding provides an additional "virtual" or covert channel of digital communications through the embedding of some secret unperceived information directly into the multimedia content without extra meta data, headers, sophisticated specialized formats and attachments. This naturally leads to the concept of a $smart\ media$ where the features of the multimedia content are extended to extra functionalities that can be exploited for multimedia processing, communications, security and content management.

The concept of a smart media can be generally characterized as:

- self-sufficient or self-embedding (no extra headers, meta data and attachments are needed);
- self-synchronizing (no synchronization information is used on the protocol side);
- self-authenticating (no access to the original data is required to establish the content authenticity);
- self-correcting and offering error concealment (no format protocol modifications related to forward/backward error corrections are necessary).

Besides the obvious advantages listed above, multimedia data hiding should additionally provide:

- perceptually invisible data embedding;
- robust and content independent extraction of embedded information;
- scalability of the content for different heterogeneous networks and applications;
- security provided by a proper key management and undetectability of the hidden data presence by the existing detection tools.

We consider multimedia data-hiding with respect to three main applications that should address the open issues presented in Section III:

- robust watermarking;
- integrity control and tamper proofing;
- secure communications.

The robust watermarking is mainly used for copyright protection, content authentication and content tracking. Integrity control and tamper proofing target verification of content integrity, detection of local modifications in images, video and documents, recovering of the original content based on available copy of the modified or tampered content. Finally secure communications address the issue of secure content delivery over the public networks using two different possibilities. The first possibility is a visual "encryption" or scrambling that should provide additional error resilience in the case of wireless networks and networks with packet losses and erasures. The second possibility is steganography that guarantees secure content delivery by hiding the content to be securely communicated into the covert media whereas the presence of the hidden content presence should not be detected by various detection tools.

V. Robust watermarking

Robust watermarking is one of the most challenging research directions of data-hiding combining a number of multidisciplinary issues ranging from information theory and digital communications, estimation and detection theory, to image processing and computer vision. Robust watermarking, from the information-theoretic perspective, should provide the reliable communication of some energy constrained payload m in the body of a multimedia content under a broad list of various intentional and unintentional attacks, those attacks constituting the resulting watermarking channel. The protocol describing robust watermarking can be schematically explained as in Figure 1. This protocol consists of three main parts, i.e., information embedding or encoder, channel that represents the public network and information extraction part or decoder.

The goal of the information embedder consists in the invisible "integration" of a specifically preprocessed payload m into the original (host) content $\mathbf{x}$ based on some secret key K. We assume that the message M, uniformly distributed over the message set $\mathcal{M}$ with the cardinality $|\mathcal{M}|$, is encoded based on a secret key into some watermark $\mathbf{w} = w^N = \{w[1], w[2], ..., w[N]\}$ and embedded into a host data (image) $\mathbf{x} = x^N = \{x[1], x[2], ..., x[N]\}$. We denote $\mathbf{x}$ to be a two-dimensional sequence typically representing the luminance of the original image. The ith element of $\mathbf{x}$ is denoted as $x[i]$ where $i = (n_1, n_2)$ and $\mathbf{x} \in \mathbb{R}^{\mathbf{N}}$ and $N = N_1 \times N_2$ is the size of the host image. The message m typically has a length of 64 bits, i.e., $|\mathcal{M}| = 2^{64}$, and is content independent. In some cases, only a binary decision about the watermark presence/absence can be required: $|\mathcal{M}| = 2$ (so-called 1-bit watermarking, i.e., $\log_2 |\mathcal{M}| = 1$ bit). As another example, the printing industry only requires 16 bits for document tracking aiming at identifying the distribution channels. In any case, the payload for robust watermarking is relatively modest and rarely exceeds 100 bits. The embedding rule can be expressed as a mapping:

$$w[i] = f_i(m, x^i), \quad (1)$$

$$y'[i] = x[i] + w[i], \quad (2)$$

where m is a particular realization of the random message M, y'_i, $1 \leq i \leq N$ is the stego data and x^i can be used only partially as $x^i = \{x[1], x[2], ..., x[i]\}$ (so-called causal side information), or entirely $x^i = \{x[1], x[2], ..., x[N]\}$ (so-called non-causal side information). We also include in this generalized model both spread spectrum schemes and host interference cancellation schemes based on pre-coding, according generally to Gel'fand-Pinsker [3], and particularly to Costa coding [4] developed for Gaussian content. The setup (1) is quite general and can include different particular cases of watermarks. For example, watermark $\mathbf{w} \in \mathbb{R}^N$ and $W[i] \sim \mathcal{N}(0, \sigma_w^2)$, i.e., zero-mean Gaussian, $\mathbf{w} \in \{\pm 1\}^N$, i.e., pseudo random binary watermark, $\mathbf{w} \in \{\{-1\}^z\{+1\}^z\}^n$, i.e., pseudo random block-repeated watermark, $\mathbf{w} \in (-\triangle/2; +\triangle/2)^N$ and $W[i] \sim \mathcal{U}(-\triangle/2; +\triangle/2)$, i.e., uniform watermark. The admissible distortion for watermark embedding is D_1:

$$E[d_1^N(\mathbf{X}, \mathbf{Y}')] \leq D_1, \quad (3)$$

where $d_1^N(\mathbf{X}, \mathbf{Y}') = \frac{1}{N}\sum_{i=1}^{N} d_1(x[i], y'[i])$ denotes $N-$vector distortion between vectors $\mathbf{X}$ and $\mathbf{Y}'$ and $d_1(x[i], y'[i])$ denotes element-wise distortion between ith elements $x[i]$ and $y'[i]$.

The channel is characterized as a transition probability $p(y|w, x)$. The channel can be quite general and include both signal processing and geometrical distortions of the stego data. In the particular case of intentional attacks, the attacker aims at removing the watermark $\mathbf{w}$ from $\mathbf{y}'$ producing the attacked data $\mathbf{y}$. The admissible attacker distortion is D_2 that is defined in the same way as (3) between vectors $\mathbf{y}'$ and $\mathbf{y}$:

$$E[d_2^N(\mathbf{Y}', \mathbf{Y})] \leq D_2. \quad (4)$$

One should also note another possibility to define the attacker distortion between the original data $\mathbf{x}$ and the attacked data $\mathbf{y}$. The decoder produces the estimate of $\hat{M}$ based on $\mathbf{y}$ using:

$$\hat{m} = g(y^N), \quad (5)$$

where $g(.)$ denotes the decoding rule and $\mathbf{y} = y^N = \{y[1], y[2], ..., y[N]\}$ is the distorted stego data. The decoding error occurs when $\hat{M} \neq M$. A particular case of generalized decoding rule $g(.)$ is the maximum a posteriory (MAP) decoding rule, which minimizes the probability of error:

$$\hat{m} = argmax_{m \in \mathcal{M}} p(m|y^N). \quad (6)$$

The cryptographic security of a robust watermarking system is considered as the system "immunity" against message removal or estimation using knowledge of the algorithms (2) and (5). The blind cryptographic attack, that can be applied without the knowledge of the secret key K, can be simply designed as an exhaustive search procedure over all possible values of the watermark $\mathbf{w}$. The number of all possible watermarks to be tested in such a way is determined by the entropy of the watermark. It is obvious, that under the constraint $E[\mathbf{w}^2] \leq D_1$ the maximum entropy of a watermark with Gaussian p.d.f. is $h(W) = \frac{1}{2}\log_2(2\pi e D_1)$. In many practical watermarking algorithms such as quantization index modulation (QIM) [5], scalar Costa scheme (SCS) [6] or distortion compensated QIM (DC-QIM), the watermark code book is structured by some binning strategies that aims at host interference cancellation (or watermark invariance to the values of host images) and invariance to the geometrical transforms. This leads to scalar or vector quantization encoding strategies that represent the regular lattices aiming at overcoming the shaping loss (to be as close as possible to Gaussian p.d.f.), and periodical watermark spatial tiling to resist against affine and projective transforms. This leads to the reduction of randomness or ambiguity at the watermark decoding. Obviously, code book structuring is known as a part of the algorithm for the attacker. However, it also reduces the entropy of the watermark as any conditioning $h(W) \geq h(W|SC)$ where SC is a structure of the code book and gives more information leakage for the attacker. Therefore, some special care should be taken to prevent this leakage and to apply the data-hiding in such a way that this leakage will not be crucial for a given application. The first attempt to formalize the security of the robust watermarking technologies has been done by Barni, Bartolini and Furon [7].

The generalized diagram from Figure 1 can be considered in a simplified version shown in Figure 2 when the channel is considered as an i.i.d. additive white Gaussian noise (AWGN) channel ($Z[i] \sim \mathcal{N}(0, \sigma_z^2)$). The channel consists of two sources. The first source models the host data $\mathbf{x}$ ($X[i] \sim \mathcal{N}(0, \sigma_x^2)$) and the second one the noise $\mathbf{z}$. Both sources are acting as an interference for the payload m. Shannon's theory states that if $\mathbf{x}$ is known at both ends, then the channel capacity is equal to its theoretical upper bound [8]:

$$C = max_{p_X(x): E[\mathbf{w}^2] \leq \sigma_w^2} I(W; Y) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_w^2}{\sigma_z^2}\right). \quad (7)$$

If $\mathbf{x}$ is not known at both ends, then it acts as a strong interference. In the case of watermarking, the host data $\mathbf{x}$ is available at the encoder. Therefore, this scheme can be considered as communication with side information available at the encoder. In this case, the problem of data hiding can be reformulated as a reliable communication of the message m over the channel with noise $\mathbf{z}$ and interference $\mathbf{x}$ being known at the encoder but not at the decoder. The most general formulation of such type of communications was considered by Gel'fand and Pinsker in 1980 in non-watermarking applications and the capacity of this scheme was found as [3]:

$$C = max_{p(u,w|x)}\left[I(U; Y) - I(U; X)\right], \quad (8)$$

where U is an auxiliary random variable. The Gel'fand-Pinsker problem has a quite simple intuitive interpretation using a random binning argument. If we denote a set of all elements (codewords) as $2^{NI(U;Y)-\varepsilon}$ and apply a random binning technique we assume that each bin (subset) associated to a particular message has $2^{NI(U;X)-\varepsilon}$ elements. It is then easy to find the total number of uniquely distinguished bins as $2^{NC+2\varepsilon} = \frac{2^{NI(U;Y)-\varepsilon}}{2^{NI(U;X)-\varepsilon}}$ that directly leads to $C = I(U; Y) - I(U; X)$.

Costa (1983) has considered the above problem in the Gaussian context and found that:

$$I(U;Y) = \frac{1}{2}\log_2 \frac{\sigma_w^2 + \sigma_x^2 + \sigma_z^2}{\frac{\sigma_w^2}{\sigma_w^2+\alpha^2\sigma_x^2}(1-\alpha)^2\sigma_x^2 + \sigma_z^2}, \quad (9)$$

$$I(U;X) = \frac{1}{2}\log_2 \frac{\sigma_w^2 + \alpha^2\sigma_x^2}{\sigma_w^2} \quad (10)$$

and $C = \frac{1}{2}\log_2\left(1 + \frac{\sigma_w^2}{\sigma_z^2}\right)$ and where the auxiliary random variable has a form of $U = W + \alpha X$ and $\alpha = \frac{\sigma_w^2}{\sigma_w^2+\sigma_z^2}$ is chosen to provide independence of $W - \alpha(W+Z)$ and $W + Z$.

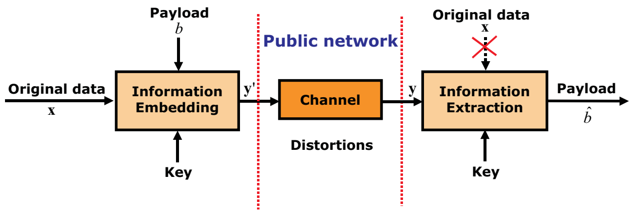


Fig. 1. Generalized diagram of robust watermarking.

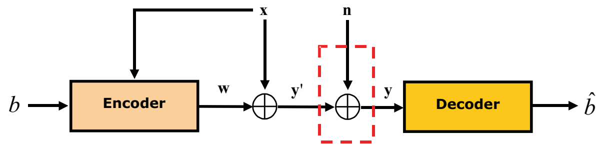


Fig. 2. Robust watermarking as communications with side information at the encoder.

Having considered the theoretical foundations of host interference cancellation using side information at the encoder, we concentrate on the practical data-hiding schemes. We will assume a binary representation of $m \equiv \mathbf{b}$ of length L_b, i.e., $\mathbf{b} \in \{0,1\}^{L_b}$. $\mathbf{b}$ is encoded into a sequence of letters $\mathbf{d}$ of length L_x with $d[i] \in \mathcal{D}$, where $\mathcal{D}$ can be binary $\mathcal{D} \in \{0,1\}$ or multilevel $\mathcal{D} \in \{1,2,...,D\}$ with $D = |\mathcal{D}|$, using some suitable error correction codes and proper spreading. Additionally, the sequence $\mathbf{d}$ can be modulated. The simplest case of modulation is M-PAM signal constellation that consists of $M \geq 2$ equidistant real symbols centered on the origin, i.e., $\mathbf{d} = \frac{d_0}{2}\{-M+1, -M+3, ..., M-1\}$ (Figure 3), where d_0 is the minimum distance between symbols. For equiprobable symbols the average symbol energy is $E_{\mathbf{d}} = E[\mathbf{d^2}] = (M^2-1)d_0^2/12$. The highest rate for the unencoded M-PAM is $R = \log_2 M$. For example, binary antipodal signaling is the particular case of 2-PAM: $M = 2$, $d_0 = 2$ and $\mathbf{d} = \{\pm\mathbf{1}\}$ and 4-PAM leads to the possible constellations $M = 4$, $d_0 = 2$ and $\mathbf{d} = \{\pm\mathbf{1}, \pm\mathbf{3}\}$.

However, contrarily to digital communications where the sequence $\mathbf{d}$ is directly used for the transmission over the noisy channel, the encoded message is combined with the host data in digital data-hiding applications according to the additive model (2). In a more general setup, the resulting watermark $\mathbf{w}$ could be:

a) $\mathbf{w} \in \mathbb{R}^N$ and $W[i] \sim \mathcal{N}(0, \sigma_w^2)$, i.e., zero-mean Gaussian or generated as an appropriate M-sequence (without error correction codes);

b) $\mathbf{w} \in \{\pm 1\}^N$, i.e., pseudo random binary unencoded watermark (particular case of 2-PAM or BPSK);

c) $\mathbf{w} \in \{\{-1\}^z\{+1\}^z\}^n$, i.e., pseudo random block-repeated watermark;

d) $\mathbf{w} \in \{\pm 1\}^N$, i.e., pseudo random binary watermark encoded by low-rate soft-decoding error correction codes;

e) $\mathbf{w} \in \{\pm 1, ..., \pm M\}^N$, i.e., pseudo random M-ary unencoded watermark (particular case of M-PAM), uniform or coded modulation watermark like trellis coded modulation (TCM).

Depending on the different embedding rules (1), we can classify all existing data-hiding techniques as those that do not use the side information about the host data at the encoder, and those that use the side information.

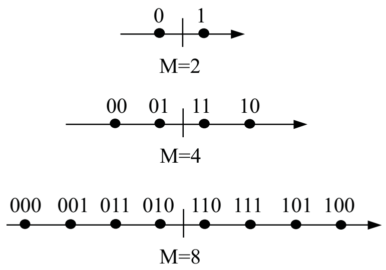


Fig. 3. M-PAM constellations.

Spread spectrum (SS) data embedding is historically the first and currently most often used technique in practice technique for data-hiding. The SS data-hiding does not directly use information about the host image for the watermark encoding and thus suffers from host interference:

$$y'[i] = x[i] + w[i], \quad (11)$$

where $\mathbf{w}$ can be any of the above techniques (a-d). However, in the most practical SS robust watermarking schemes proper spreading is applied for security, redundancy and geometrical attacks resistance reasons. This spreading is performed over the host data using a key-dependent spreading sequence $s \in \{\pm 1\}$ such that $w[j] = c[k]s[j]$, $j \in S_k$, and where $\mathbf{c}$ is the codeword of length L_c (particular case of $\mathbf{d}$ encoding) that is mapped to 2-PAM, i.e. $\mathbf{c} \in \{\pm 1\}^{L_c}$ and S_k are non-overlapping subsites that are used for the allocation of each bit of codeword $\mathbf{c}$. Additionally, the watermark can be embedded exploiting particularities of human visual system (HVS), so-called perceptual adapted watermarking:

$$y'[i] = x[i] + \gamma[i]w[i], \quad (12)$$

where $\gamma[i]$ represents a mask adapted to the HVS in the coordinate or some transform domain such as DCT, DFT or wavelets [9], [10], [11], [12], [13], [14]. In most cases, an optimal ML-detector is used for the proper stochastic model of host data $\mathbf{x}$ that takes the decision about the codeword $\hat{\mathbf{c}}$ with following appropriate soft-decoding [15], [13]. Moreover, channel state estimation can be applied to determine the distribution of channel noise, fading or erasures according to the model of binary symmetrical channels [16] or generalized channels [17] referring to diversity watermarking.

We consider 3 main variations of Costa's approach proposed for the host interference cancellation assuming data hiding with side information: Least Significant Bit Modulation (LSBM) [18], QIM [5], SCS [6].

The LSBM encoder embeds the data according to the next rule:

$$y'[i] = Q(x[i])+d[i] = x[i]+d[i]+(Q(x[i])-x[i]) = x[i]+w[i]. \quad (13)$$

The image is first precoded based on an uniform quantizer $Q(x)$ with a step Δ and then the M-PAM watermark $\mathbf{d}$ is added to this image. The embedding distortion is:

$$D_{y'x} = E[|\ \mathbf{y}' - \mathbf{x}\ |^2] = \frac{\Delta^2}{12} + E[\mathbf{b}^2] = \frac{\Delta^2}{12} + \frac{(M^2-1)d_0^2}{12}. \quad (14)$$

The LSBM decoder performs the direct estimation of the message:

$$\hat{d}[i] = y[i] - Q(y[i]). \quad (15)$$

The binary QIM encoder performs the quantization of the host image using two sets of quantizers $Q_{-1}(.)$ and $Q_{+1}(.)$ that are shifted by Δ with respect to each other:

$$y'[i] = Q_d(x[i]) = x[i]+(Q_d(x[i])-x[i]) = x[i]+w[i], \quad (16)$$

where $Q_d(.)$ denotes the corresponding quantizer for $d=-1$ and $d=+1$. The QIM embedding distortion is:

$$D_{y'x} = E[|\ \mathbf{y}' - \mathbf{x}\ |^2] = \frac{\Delta^2}{12}. \quad (17)$$

Therefore, the embedding distortion for the LSBM is higher than that for the QIM. However, it is necessary to note that the LSBM can have the same embedding distortion as the QIM, if one applies a distortion minimization procedure choosing the resulting quantization bin with the minimum possible distortion after final addition of the M-PAM watermark. This will not affect the capacity, but it will decrease the embedding distortion. The QIM decoder performs the ML-estimation:

$$\hat{d} = argmin_{d\in\{\pm 1\}} \|\ y[i] - Q_d(y[i])\ \|^2. \quad (18)$$

Contrary to the LSBM and the QIM, which do not use any prior information about the attacking channel state, the SCS exploits the knowledge of the AWGN channel statistics at the encoder. The SCS encoder generates the stego data based on the rule:

$$y'[i] = x[i] + \alpha(Q_d(x[i]) - x[i]) = x[i] + \alpha w[i]. \quad (19)$$

The parameter α is optimized to resist against the AWGN attack. It should be noted that when $\alpha = 1$ the SCS corresponds to the QIM, as well as to the case when $\sigma_z^2 \to 0$ – the high watermark-to-noise-ratio (WNR) regime. Also, a useful analogy with the channel state information about the statistics of the AWGN channel could be outlined. In particular, the variance of the noise should be known at the encoder in advance. Since it is not the case in practical applications, Eggers *et al* propose to optimize α for the working dynamic range of the $\mathbf{WNR} \in [-20, +20)$ dB [6]. This leads to a slight decrease of the performance. The SCS embedding distortion is:

$$D_{y'x} = E[|\ \mathbf{y}' - \mathbf{x}\ |^2] = \alpha^2\frac{\Delta^2}{12}. \quad (20)$$

The probabilities of error in spread spectrum and quantization-based data-hiding techniques have different characters, that drastically influence the performance of these methods in different regimes. In particular, the probability of error for the spread-spectrum based data hiding methods is computed as in digital communications for M-PAM modulation (Figure 4) including the additional impact of the host data expressed as the convolution $p_Y(y) = p_X(x) * p_Z(z) * p_D(d)$. The fundamental difference with the quantization-based techniques consists in the periodic integration of the probability of the error over all bins that do not coincide with the transmitted symbol constellation (Figure 5). Therefore, for high variance of AWGN attack, this error can increase more rapidly in contrast to the SS-based data-hiding. The reader is referred to [19] for more details about performance analysis of different data-hiding techniques under various additive attacks.

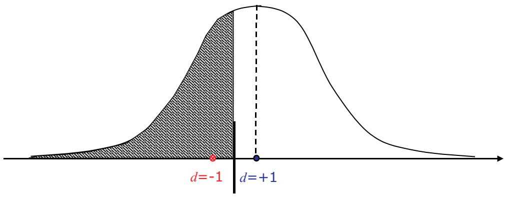


Fig. 4. Probability of error computation for $p(y|d=+1)$ and binary spread-spectrum based embedding. The highlighted region indicates the error.

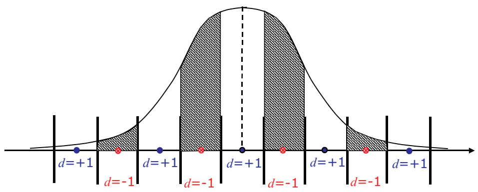


Fig. 5. Probability of error computation for $p(y|d=+1)$ and binary QIM-based embedding.

The performance of different watermark encoding and modulation (embedding) techniques can be considered depending on an operational WNR: $\mathbf{WNR} = 10\log_{10}\frac{\sigma_w^2}{\sigma_n^2}$ for AWGN channels. Low-rate data hiding achieves AWGN channel capacity in low-WNR regime while high-rate data hiding is possible for relatively high-WNR regime. The low-WNR regime is typical for robust digital watermarking when the attack is aiming at removing the watermark. In this case, the variance of the attack might be higher than the variance of the watermark. In this case, the host interference is not crucial for approaching channel capacity and spread spectrum based data-hiding can be sufficient. In this regime, two approaches to watermark encoding are mostly used in practice:

• binary watermark encoding using binary low-rate error correcting codes with soft decoding (Turbo codes, or LDPC codes);

• binary watermark encoding using the above binary codes with higher rates and following replication.

The first approach is characterized by a lower probability of error while the second one has a higher resistance against the cropping attack. It should be also noticed that the error correction codes for erasure channels can also be used to withstand cropping attack. Additionally, properly designed repetitive watermark can be also used to recover from geometrical attacks that are characterized by an affine transform, using self-synchronization [20], [21], [13], [22].

The high-WNR regime makes it possible to increase the watermark embedding rate for the same embedding distortions. In the general case, unencoded M-ary pulse amplitude modulation (PAM) can be used to approach channel capacity within 1.53 dB (that is related to a shaping loss of uniform vs. Gaussian p.d.f. of watermark). Finally, a coded modulation is used in practice that combines M-ary signaling with binary error correcting codes such as Turbo codes or LDPC codes. The host interference cancellation embedding is also necessary for this regime. Therefore, methods based on Gel'fand-Pinsker (Costa) framework should be used. However, their performance will be very poor for the low-WNR regime. Keeping in mind relatively low watermark embedding rate required for the robust watermarking applications, the SS-based methods could be recommended. Moreover, as discussed, Costa-based methods have good performance for the AWGN attack while the spectrum of all possible attacks and corresponding noise distributions is much broader in practical applications. The simple change of noise from AWGN to additive uniform noise demonstrates the very low robustness of Costa-based methods while SS-based methods are practically insensitive to the change of noise statistics even without special adaptivity of the matched detector part [19]. In addition, the question of the worst case noise (attack) is still open for the Costa-based methods and additional research is required. It is possible to foresee that the worst case attack against Costa-based methods could be based on noise with non-periodical trains of pulses that should trick the unique watermark detection. Additional attacks can be imagined where the attacker can estimate the parameters of the used quantizers in LSBM, QIM or SCS and requantize data to the original centroids $Q[x]$ providing even an enhancement of stego data quality.

A natural question arises then: where is the limit in the game between the data-hider and the attacker? Consequentially, what are the maximum data-hiding capacity and the worst attacking strategy? The estimation of data-hiding capacity for real images based on game between data hider and attacker was performed by Moulin and Mihcak [23] based on the estimation-quantization image model of LoPresto [24] and the spike model of Weidmann and Vetterli [25]. Recently, the same framework was applied to edge-process stochastic image models proposed by Voloshynovskiy $et\ al$ [26] where not so optimistic results were reported concerning the actual data hiding capacity for robust watermarking.

Most of robust watermarking schemes are vulnerable to the copy attack [27], a protocol attack which consists in the estimation of the watermark from a protected image and its re-embedding into another media, creating an ambiguity about the hold copyright.

It should also be mentioned that additional specific requirements of robust data hiding for medical and military applications exist, where the robust watermark should be reversible (i.e., completely removable with the corresponding authorization). This preserves the quality of the content and allows personalizing the content for different users. The first practical schemes of reversible watermarking were proposed by Fridrich $et\ al$ [28], [29] using LSBM-based data embedding. Obviously this sort of embedding had very low robustness. A practical scheme based on QIM embedding was proposed by Eggers $et\ al$ [30]. Kalker and Willems have performed the estimation of capacity bounds for invertible robust watermarking [31].

Summarizing the above discussion, we can point out the main requirements of robust watermarking. Robust watermarking requires the embedding of a 64-bit content independent message (low capacity) into the original image in an invisible manner specified by a proper distortion criteria. It is also required to have high robustness to all intentional and unintentional attacks and distortions both coming from signal processing and geometrical transformations. The security requirement calls for a proper resistance against message removal that would be based on the knowledge of the algorithm.

The design of practical algorithms that take into account all these conflicting requirements is a very challenging task. One of the possible examples of a practical technique based on the SS-based embedding with soft-decoding that meets these requirements is the *Berkut 1.0* technology developed at the University of Geneva [32]. *Berkut 1.0* has the best so far reported benchmarking scores according to Stirmark 3.1 (0.996). The watermark embedding is performed in a critically sampled wavelet domain with appropriate anisotropic perceptual mask that takes into account texture and luminance masking in each sub band. The robustness against geometrical attacks is ensured based on a special periodical watermark. An important issue of watermark security of periodical watermark is also resolved by increasing the watermark entropy and thus reducing the watermark predictability. The watermark is not simply repeated like it is done in the majority of SS-based techniques but it is tiled with some key-dependent predistortions in such a way that a non-authorized averaging of all tiles leads to the watermark self-destruction and thus watermark prediction is not very accurate. However, we should note that although this technology is practically very robust to all attacks from the Stirmark benchmark, there is always the possibility that soon new more powerful attacks might appear in the never ending data-hiding/attacker game.

VI. Integrity Control, Tamper proofing and Watermark-assisted Communications

The goals of integrity control and tamper proofing consists in the verification of content integrity, in the detection of local modifications in images, video and documents, in the recovering of the original content based on the available copy of modified or tampered content. The generalized block-diagram of an integrity control and verification system is shown in Figure 6. This protocol is quite similar to the robust watermarking (Figure 1) and consists of three main parts. The first part, information embedding, has the same purpose as in robust watermarking, i.e. embedding of the payload $\mathbf{b}$ into the original data $\mathbf{x}$ with the specified distortion that should not exceed D_1. However, a fundamental difference exists between these two applications that consists in the nature of the payload $\mathbf{b}$. The payload $\mathbf{b}$ has a higher rate (about 5-10 Kbits depending on the size of the original data). Moreover, the payload $\mathbf{b}$ is content dependant and related to the original data by some mapping rule $p(b|x)$ that might represent some hashing, features or even compressed version of the original content. Therefore, depending on the final requirements it might be necessary to provide the embedding rate in the range of $R = 1 - 2$ bpp (bits per pixels).

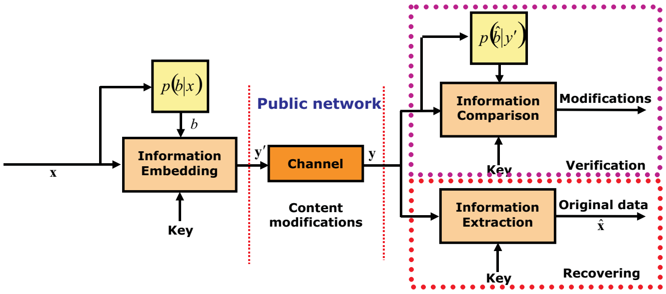
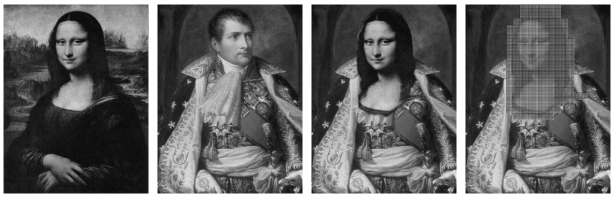


Fig. 6. Generalized diagram of integrity control, tamper proofing and self-recovering systems.

The second element of the protocol is the public network represented by some channel with the transition matrix $p(y|y')$. The behavior of this channel also shows significant differences with the corresponding robust watermarking channel. Contrarily to the robust watermarking channel, where the attacker is interested in impairing the reliable watermark detection/decoding subject to the constraint of the maximum allowable distortion D_2, the protocol attacker in this application has completely different objectives. The main goal of the attacker is to modify or to counterfeit the content with the purpose of producing a new content with a modified visual appearance. For example, the content could be modified by replacing objects, objects features, human faces, bodies, different authentication attributes, background, or any identification data targeting some sensational, misleading or illegal purposes. Obviously, in this case the document is either partially modified or a fraction of the document is copied into another document. Therefore, the global introduced distortion D_2 is of secondary importance for the evaluation of the degree of document modification for this application. The following example demonstrates the possible content modifications of two source images (Figures 7.a,b); such alterations could change the historical, artistic or even criminalistic conclusions that could be drawn. Figures 7c is the result of a collage between the two previous images. The goal of the decoder of a tamper proofing system is thus to reliably detect the intentional or unintentional modifications (Figure 7d) and to preferably reconstruct the original content.



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

Fig. 7. Example of tamper proofing: (a) and (b) original images, (c) modified content as the result of collage between (a) and (b), (d) highlighted regions indicate the content modifications.

Therefore, from the attacker perspective the integrity of the document should be preserved in such a way that the authentication watermark will not be capable to detect the introduced modifications. This is a very challenging task that recently caused a lot of attention in the watermarking community with respect to the investigation of new protocol attacks against tamper proofing systems [33]: such attacks are mostly advanced substitution attacks including the cut-and-paste attack [34], the vector-quantization (VQ) or Holliman-Memon attack [35], collage and composition attacks, as well as cryptographic attacks targeting hash-codes such as the birthday attack [36].

To withstand the above attacks one should properly design a data-hiding scheme that should resolve two related problems:

- detection of modifications;
- recovering of the original data $\mathbf{x}$ after content modifications.

According to the payload and the targeted objectives, the existing practical systems can be divided in three large groups:

- visual hashing;
- hybrid robust watermarking and tamper proofing;
- self-recovering watermarking.

A. Robust visual hashing

The idea of robust visual hashing is to generate a key-dependent secure digest which continuously changes with the input, differing at most by a small number of bits for two distinct but perceptually equivalent inputs. Robust hashing can be seen as a three-steps operation: first, *features extraction* which resists to the transformations that we define as acceptable; secondly, a (generally key-dependent) *randomization* process on these features in order to achieve security; thirdly, a data reduction step which maps the randomized information to a shorter bit string representing the input data.

For the features extraction step from the visual input $\mathbf{x}$, we have to define what is an "acceptable" alteration, and which inputs can be considered as "perceptually equivalent". This aspect concerns both the type and the level of distortion we want to allow, and is obviously dependent on the targeted application. Permitted distortions could include signal processing changes such as slight lossy compression, signal fading, noise addition, grey-scale conversion, etc. as well as some classes of geometrical distortions. The selected features should be robust and invariant to the allowed distortions. Early tolerant visual hashing for images have been proposed by Schneider and Chang [37] which uses features like edges, color/gray-scale histograms or DCT, and by Brandt and Lin [38] which are also robust to translation, rotation, and scaling. Xie and Arce [39] extract edges information using the DWT. Bhattacharjee and Kutter [40] extract perceptually interesting feature points that are not embedded within the image but are stored separately. Later Hel-Or *et al* [41] proposed geometric hashing based on salient points and voting algorithm, and Fridrich [42] proposed a function using the low-pass of DCT coefficients, which can be made invariant to translation, scaling and rotation using the Fourier-Mellin transform [43].

The randomization step generally based on a key K is essential, since the generated code should keep the same properties as a classical cryptographic hash function beside their continuous character: codes should be unpredictable for random inputs, and two completely different inputs should result into uncorrelated codes. In the case of keyed hashing, two different keys (differing even by a single bit) should also produce totally different codes. Fridrich [42] uses key-dependent random matrices to randomize low-pass DCT, and Venkatesan *et al* [44] propose a random tiling of the wavelet transform (DWT) of the input prior to features extraction.

Finally the data reduction step is the irreversible data compression which reduces the length of the encoded features to a compact digest code. Both the randomization and the data reduction steps should preserve the continuous property of the input features, and for this purpose these two last steps could be done together rather than separately.

The verification is then done by counting the percentage of mismatching bits with a threshold representing the amount of allowed distortion.

B. Hybrid robust watermarking and tamper proofing

While robust watermarking for copyright protection was clearly the first main research direction of the $90th$, authentication and tamper proofing watermarks have then been rapidly proposed for authentication and verification of integrity. Authentication aims at checking the authenticity of a document and of its source, while tamper proofing is used to detect unauthorized modifications. Fragile and semi-fragile watermarks aim at making falsifications and unauthorized modifications easy to detect and characterize.

While authentication/tamper proofing watermarks generally easily detect simple local alterations, many proposed fragile schemes based on block-wise independent hashing are vulnerable to substitution attacks which use images which are protected with the same key: parts are cut from these protected images, and pasted together to form a new image – this is called the cut-and-paste attack. Generally the attacker needs to preserve some synchronization between the pasted parts in order to fool the tampering detector. The VQ or Holliman-Memon attack [45] is a cut-and-paste attack which aims at constructing completely arbitrary images which are wrongly authenticated, composed with blocks (the same blocks as those used by the tamper proofing watermark) taken from a database of images protected with the same key; this attack results in very good quality faked images. Various methods of neighboring blocks and hash-codes chaining can defeat the VQ attack. However in a collage attack larger parts are cut from the source images; in this case each pasted area is individually authenticated by the detector, and only the boundaries between them are detected. This makes it difficult to figure out the actual authenticity of the copied regions with respect to each other in the context of the composed image, and a collage cannot be distinguished with certainty from simple local tampering. Therefore the collage attack can be seen as a protocol attack resulting into an ambiguity about the partial authenticity of the image and the nature of the applied attack. No classical tamper proofing watermarking scheme is able to solve this problem, except the one of Fridrich [46] which proposes to embed an additional unique ID (e.g. time-stamps) within each image, or each hashed block.

Regarding robust watermarking, the copy attack is also a protocol attack creating the ambiguity by copying a watermark from a protected image to another one. This is a potential problem for many real-world applications: how to be sure that the document holds the real copyright message? While several approaches have been proposed to defeat this attack, one possibility is to include host data related information into the watermark in order to detect the copy attack. However we propose a more powerful solution consisting of joining a robust watermark and a tamper proofing watermark in a hybrid approach. First, a hybrid scheme can solve copyright problems and check authenticity and integrity in an integrated approach. Secondly, this is of great advantage for defeating the two protocol attacks mentioned above: the copy attack and the collage attack. The copy attack is made impossible since hash-codes immediately fail at the verification stage if the watermark was copied to another host. Regarding the collage attack, the robust part of the hybrid watermark helps us to determine if the image is made of different areas coming from different sources (holding different robust watermarks), and to distinguish between these areas. Fridrich [46] proposed such a hybrid method, but she uses a watermark with relatively low robustness of the robust part, and the advantages of the hybrid concept against these two protocol attacks were not indicated.

Our hybrid watermark scheme, described in more details by Deguillaume *et al* [33], works as follows: first, a highly robust watermark is integrated with a fragile or semi-fragile block-wise watermark for combined copyright protection, tamper proofing and authentication. Secondly, the fragile/semi-fragile part is embedded orthogonally with respect to the robust part in order to fully preserve it; this orthogonality is obtained by placing both watermarks at different positions (meaning different pixels). Thirdly, additional cryptographic countermeasures, such as hash-codes and blocks chaining, unique time-stamps, undeterministic hash-codes, etc. are used in order to defeat substitution attacks. Finally, the information coming from both the robust and the fragile/semi-fragile parts are combined and interpreted in order to detect copy or collage attacks. This solution is integrated in a prototype *Berkut 2.0* [32].

C. Self-recovering watermarking

Error resilient coding and error concealment have received recently a lot of attention in different application related to wireless networks and networks with no QoS control. The main existing techniques can be characterized as [47] : layered coding with transport coding, multiple description coding, joint source/channel coding, robust waveform coding, robust entropy coding and post-processing at the decoder. Data-hiding techniques could be used as well for this purpose. Moreover, intentional content modifications could be considered as the channel degradation and appropriate strategies can be applied for the self-recovering data.

The main practical approaches to self-recovering watermarking differ depending on the used payload (features, edges, compressed coefficients), data-embedding technique and final reconstruction/recovering procedure. For instance, an example of edge directivity embedding is proposed by Yin *et al* [48] while downsampled and lossy compressed (JPEG QF=25) payload is used in SARI technique [49].

Generally, any sort of image features can be embedded into the image itself that should help reconstruct the resulting image after channel degradations. If the quadratic distortion is used as a fidelity measure and the channel distortions are interpreted as AWGN, and if the content is assumed to be stationary Gaussian, one can apply the MMSE estimator to reconstruct the original image (as post-processing). The resulting variance of the obtained estimate σ^2_{MMSE} depends on the variance of the content σ^2_x and the variance of the channel noise σ^2_z, as: $\sigma^2_{MMSE} = \frac{\sigma^2_x \sigma^2_z}{\sigma^2_x + \sigma^2_z}$. Therefore, the higher the variance of the image, the lower is the accuracy of the estimate. A maximum likelihood (ML) estimate is most often applied to real images to estimate the local image variance. It is a known fact that real images are highly non-stationary processes. The variance in the vicinity of the edges and textures will thus be highly overestimated [50], σ^2_{MMSE} will then be very large in these regions and no reliable estimate will be possible. Therefore, one can embed additional information about edges and textures in the watermark to reduce the variance of the estimation, while flat regions that are characterized by relatively low variance can easily be reconstructed at the decoder. This approach to error-resilient coding can be efficiently used for the SoQ control and enhanced scalability of public networks.

D. Joint source/channel coding with side information

All the above schemes can be considered in a generalized setup of joint source/channel coding with side information. Since we have already considered channel coding with side information at the encoder in Section V, we will focus in this section on source coding with side information at the decoder.

We start by considering the problem of lossy compression with side information (Figure 8). This problem was first introduced by Wyner-Ziv (1976) [51] with $\mathbf{X}$ and $\mathbf{Y}$ being continuous correlated i.i.d. sources with joint p.d.f. $p_{XY}(x,y)$. The problem is to compress $\mathbf{X}$ in a lossy way with $\mathbf{Y}$ being known at the decoder but not at the encoder. First, we consider this problem for a Gaussian content and quadratic distortion. The source $\mathbf{X}$ produces N samples with $X[i] \sim \mathcal{N}(0, \sigma^2_x)$. The encoder and the decoder communicate without error at a rate R bits per source symbol. At the same time, the decoder has access to $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$ (Figure 9), where $\mathbf{X}$ and $\mathbf{Z}$ are independent and $Z[i] \sim \mathcal{N}(0, \sigma^2_z)$. The goal is to communicate with the lowest possible rate R such that $E[d^N(\mathbf{X}, \hat{\mathbf{X}})] \leq D$. This lower bound will be denoted as $R(D)^{WZ}_{X|Y}$.

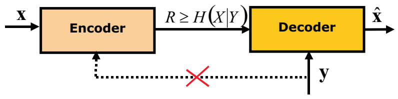


Fig. 8. Generalized diagram of lossy source coding with side information $\mathbf{y}$.

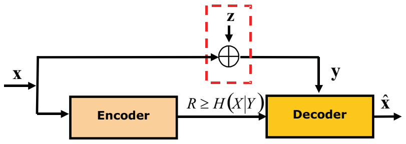


Fig. 9. Generalized diagram of lossy source coding with side information given in the form of a noisy version of $\mathbf{x}$: $\mathbf{y} = \mathbf{x} + \mathbf{z}$.

This communication protocol is based on the fact that if both encoder and decoder have access to $\mathbf{Y}$, then they can compute a minimum mean square error (MMSE) estimate of $\mathbf{X}$ as $\mathbf{X}_{MMSE} = E[\mathbf{X}|\mathbf{Y}]$. In this case one can only communicate the error of estimate $\tilde{\mathbf{X}} = \mathbf{X}_{MMSE} - \mathbf{X}$ ($\tilde{X}[i] \sim \mathcal{N}(0, \sigma^2_{X|Y})$), where $\sigma^2_{X|Y} = \frac{\sigma^2_x \sigma^2_z}{\sigma^2_x + \sigma^2_z}$, with the specified distortion D, that corresponds to a rate distortion function $R(D)_{X|Y}$ which assumes $\mathbf{Y}$ to be available at both encoder and decoder:

$$R(D)_{X|Y} = \begin{cases} \frac{1}{2} \log_2 \frac{\sigma^2_{X|Y}}{D}, \text{ if } 0 \leq D < \sigma^2_{X|Y} , \\ 0, \ D > \sigma^2_{X|Y}. \end{cases} \tag{21}$$

Wyner and Ziv [51], [52] demonstrated that generally $R(D)^{WZ}_{X|Y} \geq R(D)_{X|Y}$. This means that there is in general a rate loss with Wyner-Ziv coding. Zamir [53] also shown that this loss can be as close as $R(D)^{WZ}_{X|Y} - R(D)_{X|Y} \leq \frac{1}{2}$ bit. Note that for discrete sources when $D = 0$, the Wyner-Ziv problem reduces to the Slepian-Wolf problem [54] with $R(0)^{WZ}_{X|Y} = R(0)_{X|Y} = H(X|Y)$. The generalized rate distortion with side information at the decoder for discrete memoryless sources with distortion measure $d(.,.)$ was considered in [8], [51], [52]:

$$R(D)^{WZ}_{X|Y} = min_{p(u|x),g(.)} \left[I(X;U) - I(Y;U) \right]. \tag{22}$$

The minimization is performed over all $p(x,y,u) = p(x,y)p(u|x)$ and all decoder functions $\hat{x} = g(u,y)$ such that $\sum_{x,u,y} p(x,y)p(u|x)d(x,g(u,y)) \leq D$.

Su *et al* [55] also shown alternatively that for $U^*[i] \sim \mathcal{N}(0, \sigma^2_u)$ where $\sigma^2_u = (\sigma^2_x - \frac{\sigma^2_x + \sigma^2_z}{\sigma^2_z} D)\frac{\sigma^2_z - D}{\sigma^2_z}$ one can obtain:

$$I(X;U^*) = \frac{1}{2} \log_2 \frac{(\sigma^2_z - D)\sigma^2_x}{\sigma^2_z D}, \tag{23}$$

$$I(Y;U^*) = \frac{1}{2} \log_2 \frac{(\sigma^2_z - D)(\sigma^2_z + \sigma^2_x)}{(\sigma^2_z)^2}, \tag{24}$$

such that the rate $R^* = I(X;U)^* - I(Y;U)^* = R(D)_{X|Y}$.

The design of the code book $\mathcal{U}$ is quite similar to the Gel'fand-Pinsker code book construction and includes about $2^{NI(X;U^*)-\varepsilon}$ vectors coming from $\mathcal{N}(\mathbf{0}, \sigma_u^{*2}\mathbf{I})$. The vectors are equiprobably randomly assigned to $2^{N(R^*+2\varepsilon))}$ distinct bins with some indexes and each bin contains about $2^{NI(Y;U^*)-\varepsilon}$ vectors.

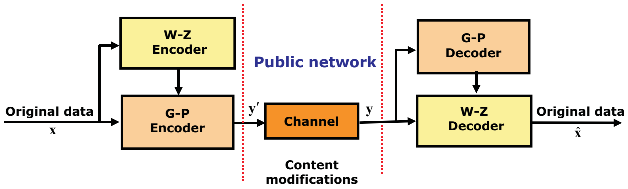


Fig. 10. Generalized block-diagram of joint source/channel coding based on side information.

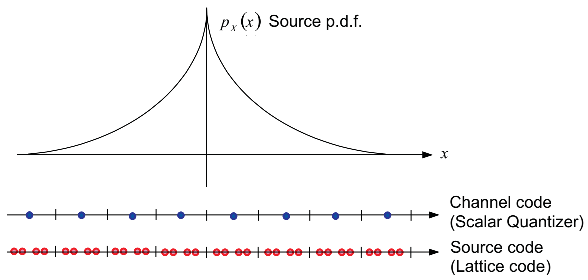


Fig. 11. Joint source/channel coding based on side information.

Having considered the main results of source and channel coding with side information, we can design a joint source/channel coding (JSCC) system that generalizes the above approaches. The block diagram of JSCC system with side information is shown in Figure 10. For simplicity, assume that the channel is characterized either by AWGN or by some high-rate lossy compression that degrade the image quality. The allowable channel distortion is D_2 while the degradation due to the watermark embedding should not exceed D_1. The ratio D_1/D_2 determines the maximum data-hiding rate according to the Gel'fand-Pinsker (8), Costa (9), and (10) channel coding setups. The source coding in the above JSCC scheme is designed assuming the Wyner-Ziv formulation, that is availability of the degraded stego data $\mathbf{y}$ as the side information at the decoder. The watermark (payload) represents the direct compressed channel transmission in the Wyner-Ziv problem communicated with the rate $R \geq H(X|Y)$. The simplest 1-D interpretation of the above scheme is shown in Figure 11. The channel code is represented by a uniform scalar quantizer that at the same time corresponds to a "coarse" approximation of the source data $\mathbf{x}$. The source code is designed based on a lattice code with respect to the above scalar quantizer, assuming amplitude limited attacks or distortions. In particular, 4-PAM is used within each bin of lattice code providing a total embedding rate of 2 bits per pixel. It is also assumed that the watermark is encoded according to the Wyner-Ziv problem, modulated using multilevel codes and properly allocated over the image.

The decoder extracts the watermark based on the Gel'fand-Pinsker decoding. Then the Wyner-Ziv decoder performs the reconstruction of the original data $\mathbf{x}$ using the estimated payload $\hat{\mathbf{b}}$ and the side information $\mathbf{y}$. In the noise-free case, the quality of the reconstructed image will be determined by the specified distortion D of the lossy Wyner-Ziv coding. In the case of AWGN, the ratio of half of the distance between lattice constellations ($d_0/2$) in the source code to the noise standard deviation (σ_z^2) will determine the corresponding probability of decoding error. If $d_0/2 >> \sigma_z^2$, one can expect error-free communications typical for the QIM-like schemes and corresponding reconstruction with the distortion not exceeding D. Otherwise, errors might occur and the system fails to reconstruct the original data with the given fidelity.

The above JSCC scheme can also be used as a self-recovering system for networks with bit, block or packet losses or erasures. In these case, the payload should be decreased to enable appropriate encoding using error correction codes suited to the erasure channels, or simply using appropriate data allocation with repetitions. This sort of communications represents a form of error resilient coding that can assist the problem of QoS control in public networks.

It should also be mentioned the possibility of hybrid analog/digital transmission where the digital counterpart (embedded watermark) can be used to provide additional quality of transmission for the authorized users [56].

An extension to the above JSCC is possible in the case of data delivery with a given targeted data quality to different users, that are divided on public users (those who do not know the key) and private users (those who have access to the key). Increasing the embedding distortion D_1, one can considerably degrade the image/video/audio quality thus making it uninteresting to public users, while private users can still decode the encoded data. Therefore, this scheme can also be used in applications that require "partial data encryption" to enable the secure content delivery to the target users.

VII. Secure Communications

The goal of secure communications is to securely deliver some content over the public networks. There are several possibilities for secure communications. The first one is a visual "encryption" or scrambling that should provide additional error resilience in the case of wireless networks and networks with packet losses and erasures. The second possibility is steganography that guarantees secure content delivery by hiding the content to be securely communicated into the covert media, whereas the presence of the hidden content presence should not be detected by various detection tools.

A. Visual scrambling

The goal of visual scrambling consists in the enciphering of visual content in a way suitable for reliable communications over public networks; this prevents access of a third unauthorized party to the enciphered content. The block diagram of visual scrambling is shown in Figure 12. The content that should be securely communicated over public networks is scrambled at the encoder based on the private key in such a way that it cannot be anymore visually recognized. Contrarily to traditional data enciphering, it is required here to ensure both the visual scrambling and the error resilient coding. Moreover, to provide a secure solution it is required to avoid additional redundancy in headers, meta data and attachments. It is also preferable to provide format independency and to ensure high efficiency towards erasure channels and channels with varying parameters. Obviously, traditional means cannot completely satisfy these requirements. The network part of communications is concerned in this application with two different issues, i.e., security and robustness. The security assumes that unauthorized deciphering can be applied and the robustness issue refers to different imperfections of networks explained in Section II. Finally, the decoder should provide reliable descrambling of the content even if some bits, blocks or packets have been corrupted during transmission. One of possible solutions of this problem was proposed by Grytskiv *et al* [57], based on phase encryption. This approach, while being very simple, demonstrates high efficiency for both content scrambling and error resilience.

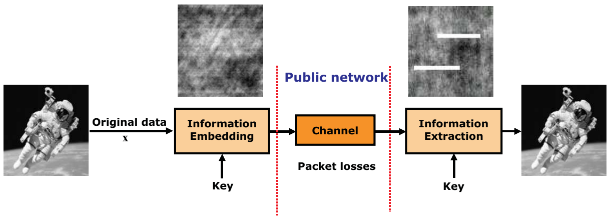


Fig. 12. Generalized diagram of visual scrambling.

B. Steganography

Steganography, originally designed for cover or hidden communications, should provide a certain level of security for public communications. The block diagram of steganographic communications is shown in Figure 13. The encoding/decoding part of steganography systems has a lot in common with robust watermarking based on Costa's scheme. However, it has reduced requirements towards attacks aiming at the watermark removal and thus it can provide higher embedding rate. It essentially corresponds to high WNR-regime of data hiding meaning that normally it should withstand unintentional attacks such as format conversion, slight lossy compression and in some special cases analog to digital conversion. While most existing steganographic tools can provide perceptually invisible data hiding, the stochastic visibility or unauthorized detectability of hidden data still remains a challenging task. Therefore, to be secure, the steganographic system should satisfy a set of requirements. The main requirement consists in providing the statistical indistinguishability between the cover data and the host data. A possible information-theoretic measure of stochastic closeness is the relative entropy or Kullback-Leiber distance (KLD) between two distributions under test, which was first proposed by Cachin [58]. More generally, the stochastic visibility can be considered as the possibility of unauthorized detection to differentiate between the cover and the host data based on a hypothesis testing.

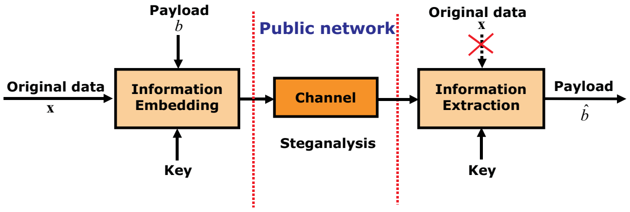


Fig. 13. Generalized diagram of secure communications based on steganography.

We review here the main countermeasures that can be used to decrease the stochastic visibility of a watermark. The main idea of these countermeasures consists in the preservation of the statistical properties of the cover data, i.e., in the design of a data hiding technology with minimum possible stochastic distortions. The main countermeasures are:

- to reduce the amount of modifications in the cover data, i.e., embedding. This will decrease the embedding rate;
- to reduce the amount of modifications by applying some error correction codes with the error correction possibility corresponding to the amount of unchanged inappropriate data;
- to reduce the amount of distortions by applying data hiding in some transform domain where the amount of zero and non-zero coefficients might not be equiprobable due to decorrelation and energy compaction properties of the applied transform. Use the ECCs that produce the resulting codewords with corresponding statistics;
- to apply encoding that uses the prior information about the host data as a side information at encoder;
- to apply a transform that corrects the statistics of stego data but preserves capacity (for example preserve relative entropy or p.d.f. or bit-plane relationships);
- to use content-based embedding assuming a non-stationary Gaussian model of cover data, i.e., the model with locally smoothly changing variance. This will provide the possibility to embed more data in the textured areas which both perceptually and stochastically are less predictable, and better preserve original content and hide modifications;
- to choose the cover image from the set of images that provides the highest level of stochastic invisibility for a given message; synthesize a composite cover data for the same purpose.

The basic scheme for steganography communications requires high-rate communications. Thus, the host interference cancellation issue should be resolved. The first steganographic techniques have been mostly built based on the LSBM embedding. The QIM and SCS based embedding for steganographic purposes, proposed by Eggers *et al* [59] and Guillon *et al* [60], have proven that the SCS-based steganography is secure according to the Cachin's criteria of ϵ-security [58] which requires:

$$D(p_X||p_Y) < \epsilon, \tag{25}$$

where $D(p_X||p_Y) = \sum_{x\in\mathcal{X}} p_X(x) \log \frac{p_X(x)}{p_Y(x)}$ denotes relative entropy (or Kullback-Leibler distance) between the cover data

X and the stego data Y.

However, the relative entropy is a global criteria and does not reflect the local content modifications. This means that the content can be modified locally in such a way that the attacker can detect it either visually or using some specially designed statistical tests, while the relative entropy can be tuned to be very low. This also valid for the estimation of image quality using the MSE criterion. It was also shown that images can be considerably locally distorted while the MSE indicated acceptable image quality [61].

At the same time, it is obvious that the higher the data embedding rate, the more modifications are introduced into the original content and consequently the easier the task of steganalysis. The trade-off between data-hiding capacity and security of data hiding technologies expressed as the possibility of unauthorized detection was performed by Voloshynovskiy and Pun [62]. Different data hiding techniques have been considered for both low-WNR and high-WNR regimes and corresponding statistical detection strategies have been proposed. It was emphasized that the crucial role in the unauthorized detection of hidden data belongs to the proper stochastic modeling of the cover content. The commonly used EQ model provides overestimated values of local image variances indicating "high steganographic security of specific image regions". Therefore, the corresponding conclusion is that one should embed the payload in edges an textures due to their high variance and corresponding high probability of error of unauthorized detection. Recent results obtained for capacity of robust data hiding techniques question the validity of these assumptions [26]. It is also likely that the appearance of new more powerful and accurate stochastic image models can change this belief and inspire new secure data hiding strategies.

VIII. Conclusion

The goal of this paper was to demonstrate how network security, QoS control and secure communications over the public networks can benefit from data hiding technologies. It was shown that such technologies can play an important assisting role in public networks characterized to be heterogeneous, time-varying, and in networks with no QoS control. We have also indicated that traditional means of multimedia security can hardly cope with novel emerging requirements of multimedia communications. The data-hiding technologies, being a possible alternative, do not require considerable investment, protocol modifications and are compatible with the existing standards of multimedia compression and communications. We have also developed a unified theoretical basis of digital data-hiding as well as shown its major applications. In particular, digital communication with side information was demonstrated to be an appropriate theoretical basis for considering different aspects of channel coding and source coding in data-hiding applications. The recent interest towards the Gel'fand-Pinsker and Wyner-Ziv problems makes it possible to consider digital data-hiding in the scope of multi-terminal and multi-user networks and communications. This makes the analysis even more attractive with a huge future potential of extensions towards multimodal data storage, communications and management in highly distributed environments. State-of-the-art robust watermarking, tamper proofing, watermark-assisted multimedia processing and secure communications are considered among others based on a unified theoretical basis. The main requirements, design principles, generalizations, as well as future perspectives are underlined in the paper.

Acknowledgment

This paper was partially supported by SNF grant No 21-064837.01, SNF Professorship grant No PP002-68653/1, CTI-CRYMEDA-SA and IM2 projects. The authors are thankful to Yuriy Rytsar for many helpful and interesting discussions.

References

[1] E. Lin, C. I. Podilchuk, T. Kalker, and E. Delp, "Streaming video and rate scalable compression: What are the challenges for watermarking?" in *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents III*, vol. 4314, San Jose, CA, USA, January 2002.

[2] S. Voloshynovskiy, A. Herrigel, Y. Rytsar, and T. Pun, "Stegowall: Blind statistical detection of hidden data," in *In E.J. Delp and P. W. Wong eds., Proccedings of SPIE Photonics West, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, San Jose, CA, USA, January 2002.

[3] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[4] M. Costa, "Writing on dirty paper," *IEEE Trans. on Information Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[5] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Information Theory.*, vol. 47, pp. 1423–1443, May 2001.

[6] J. Eggers, J. Su, and B. Girod, "A blind watermarking scheme based on structured codebooks," in *Secure images and image authentication, IEE Colloquium*, London, UK, April 2000, pp. 4/1–4/6.

[7] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," *Signal Processing, Special Issue on Security of Data Hiding Technologies*, 2003.

[8] T. Cover and J. Thomas., *Elements of Information Theory.* Wiley and Sons, New York, 1991.

[9] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, May 1998.

[10] M. S. Kankanhalli and R. K. R. Ramakrishnan, "Content based watermarking of images," in *Multimedia and Security Workshop at ACM Multimedia'98, Bristol, U.K.*, September 1998.

[11] J. F. Delaigle, C. De Vleeschouwer, and B. Macq, "Watermarking algorithm based on a human visual model," *Signal Processing*, vol. 66, pp. 319–335, 1998.

[12] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Third International Workshop on Information Hiding*, September 29 - October 1st 1999, pp. 212–236.

[13] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Content adaptive watermarking based on a stochastic multiresolution image modeling," in *Tenth European Signal Processing Conference EUSIPCO2000*, Tampere, Finland, September 2000.

[14] J.-F. D. M. Bertran and B. Macq, "Some improvements to HVS models for fingerprinting in perceptual decompressors," in *IEEE Int. Conf. on Image Processing ICIP2001*, Thessaloniki, Greece, October 2001, pp. 1039–1042.

[15] F. Pérez-González, J. R. Hernández, and F. Balado, "Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications," *Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking*, vol. 81, no. 6, pp. 1215–1238, 2001.

[16] D. Kundur and D. Hatzinakos, "Improved robust watermarking through attack characterization," in *Optics Express*, vol. 3, December 1998, pp. 485–490.

[17] S. Voloshynovskiy, F. Deguillaume, S. Pereira, and T. Pun, "Optimal diversity watermarking with channel state estimation," in *IS&T/SPIE's Annual Symposium, Electronic Imaging 2001: Security and Watermarking of Multimedia Content III*, vol. 4134, San Jose, California USA, 21-26 January 2001, pp. 23–27.

[18] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Data hiding for video-in-video," in *IEEE Int. Conf. on Image Processing ICIP1997*, vol. 2, Piscataway, USA, October 1997, pp. 676–679.

[19] F. Pérez-González, F. Balado, and J. R. Hernández, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery*, vol. 51, no. 4, April 2003.

[20] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Method for the estimation and recovering of general affine transforms in digital watermarking applications," in *IS&T/SPIE's 14th Annual Symposium, Electronic Imaging 2002: Security and Watermarking of Multimedia Content IV*, vol. 4675, San-Jose, CA, USA, January 20-25 2002, pp. 313–322.

[21] M. Kutter, "Watermarking resistent to translation, rotation and scaling," in *Proc. SPIE Int. Symp. on Voice, Video, and Data Communication*, vol. 3528, Boston, U.S.A., November 1998, pp. 423–431.

[22] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlinear geometrical distortions," in *IEEE Int. Conf. On Image Processing ICIP2001*, Thessaloniki, Greece, October 2001, pp. 999–1002.

[23] P. Moulin and M. K. Mihcak, "A framework for evaluating the data-hiding capacity of image sources," *IEEE Trans. on Image Processing*, vol. 11, no. 9, pp. 1029–1042, September 2002.

[24] S. LoPresto, K. Ramchandran, and M. Orhard, "Image coding based on mixture modeling of wavelet coefficients and a fast estimation-quantization framework," in *Data Compression Conference 97*, Snowbird, Utah, USA, 1997, pp. 221–230.

[25] C. Weidmann and M.Vetterli, "Rate-distortion analysis of spike processes," in *Data Compression Conference*, Snowbird, USA, March 1999.

[26] S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "Data hiding capacity-security analysis for real images based on stochastic non-stationary geometrical models," in *IS&T/SPIE's Annual Symposium, Electronic Imaging 2003: Image and Video Communications and Processing V*, Santa Clara, California USA, 20-24 January 2003.

[27] M. Kutter, S. Voloshynovskiy, and A. Herrigel, "Watermark copy attack," in *IS&T/SPIE's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II*, vol. 3971, San Jose, California USA, 23–28 jan 2000.

[28] J. Fridrich and M. Goljan, "Images with self-correcting capabilities," in *IEEE International Conference on Image Processing Proceedings ICIP'99*, Kobe, Japan, October 25-28 1999, pp. 792–796.

[29] ——, "Protection of digital images using self embedding," in *Symposium on Content Security and Data Hiding in Digital Media*, New Jersey Institute of Technology, USA, May 1999.

[30] J. Eggers, R. Buml, R. Tzschoppe, and B. Girod, "Inverse mapping of scs-watermarked data," in *Eleventh European Signal Processing Conference (EUSIPCO'2002)*, Toulouse, France, September 3-6 2002.

[31] F. M. W. T. Kalker, "Capacity bounds and code constructions for reversible data-hiding," in *IS&T/SPIE Proceedings, Security and Watermarking of Multimedia Contents V*, vol. 5020, Santa Clara, California, USA, January 2003.

[32] U. of Geneva Stochastic Image Processing (SIP) Group, "SIP Watermarking Technology," http://watermark.unige.ch/wmg_technology.html.

[33] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack," *Signal Processing, Special Issue on Security of Data Hiding Technologies*, 2003.

[34] P. S. L. M. Barreto, H. Y. Kim, and V. Rijmen, "Toward a secure public-key blockwise fragile authentication watermarking," in *IEEE ICIP2001*, Thessaloniki, Greece, October 2001, pp. 494–497.

[35] M. Holliman and N. Memon, "Couterfeting attacks on oblivious block-wise independant invisible watermarking schemes," in *IEEE Trans. on Image Processing*, vol. 9, no. 3, March 2000, pp. 432–441.

[36] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, October 1996.

[37] M. Schneider and S. Chang, "A robust content based digital signature for image authentication," in *Proceedings of the IEEE International Conference on Image Processing*, Lausanne, Switzerland, September 1996, pp. 227–230.

[38] R. D. Brandt and F. Lin, "Representations that uniquely characterize images modulo translation, rotation, and scaling," *Pattern Recognition Letters*, vol. 17, pp. 1001–1015, 1996.

[39] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," in *IEEE Int. Conference on Image Processing 98 Proceedings*, Chicago, Illinois, USA, October 1998.

[40] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in *IEEE Int. Conference on Image Processing 98 Proceedings*. Chicago, Illinois, USA: Focus Interactive Technology Inc., October 1998.

[41] H. Hel-Or, Y. Yitzhaki, and Y. Hel-Or, "Geometric hashing techniques for watermarking," in *ICIP 2001*, 2001, p. Watermarking i.

[42] J. Fridrich, "Visual hash for oblivious watermarking," in *IS&T/SPIE Proceedings*, vol. 3971, San Jose, California, USA, January 2000.

[43] J. J. K. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *IEEE Int. Conf. on Image Processing ICIP1997*, Santa Barbara, CA, USA, October 1997, pp. 536–539.

[44] R. Venkatesanan, S. Koon, M. Jacubowski, and P. Moulin, "Robust image hashing," in *ICIP 2000*, Vancouver, BC, Canada, September 2000.

[45] M. Holliman and N. Memon, "Counterfeiting attacks on linear watermarking systems," in *Proc. IEEE Multimedia Systems 98, Workshop on Security Issues in Multimedia Systems*, Austin, Texas, June 1998.

[46] J. Fridrich, "A hybrid watermark for tamper detection in digital images," in *ISSPA'99 Conference*, Brisbane, Australia, August 1999.

[47] Y. Wang and Q.-F. Zhu, "Error control and concealment for video communications: a review," *Proc. IEEE*, vol. 86, no. 5, 1998.

[48] P. Yin, B. Liu, and H. Yu, "Error concealment using data hiding," in *IEEE Int. Conf. On ASSP*, Salt Lake City, USA, May 2001.

[49] C. Lin, D. Sow, and S. Chang, "Using self-authentication-and-recovery images for error concealment in wireless environments," in *SPIE IT-Com/OptiComm*, vol. 4518, Denver, CO, USA, August 2001.

[50] S. Voloshynovskiy, O. Koval, and T. Pun, "Wavelet-based image denoising using non-stationary stochastic geometrical image priors," in *IS&T/SPIE's Annual Symposium, Electronic Imaging 2003: Image and Video Communications and Processing V*, Santa Clara, California USA, 20-24 January 2003.

[51] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Information Theory*, vol. 22, no. 1, pp. 1–10, January 1976.

[52] A. Wyner, "The rate-distortion function for source coding with side information at the decoder-ii: General sources," *Information and Control*, vol. 38, pp. 60–80, 1978.

[53] R. Zamir, "The rate loss in the wyner-ziv problem," *IEEE Trans. Information Theory*, vol. 19, pp. 2073–2084, November 1996.

[54] D. Slepian and J. Wolf, "Noiseless encoding of correlated information sourcea," *IEEE Trans. Information Theory*, vol. 19, pp. 471–480, July 1973.

[55] J. Su, J. Eggers, and B. Girod, "Channel coding and rate distortion with side information: Geometric interpretation and illustration of duality," *Submitted to IEEE Trans. on Information Theory*, May 2000.

[56] R. Puri, K. Ramchandran, and S. S. Pradhan, "On seamless digital upgrade of analog transmission systems using coding with side information," in *Allerton Conf. Communication, Control, and Computing*, Allerton, IL, USA, October 2002.

[57] Z. Grytskiv, S. Voloshynovskiy, and Y. Rytsar, "Cryptography and steganography of video information in modern communications," in *Proc. 3rd International Conference on Telecommunications in Modern Satelite, Cable and Broadcasting Services TELSIKS'97*, vol. 1, Nis, Yugoslavia, October 1997, pp. 164–167.

[58] C. Cachin, "An information-theoretic model for steganography," in *Information Hiding: Second International Workshop IHW'98*, Portland, Oregon, USA, April 1998.

[59] J. Eggers, R. Buml, and B. Girod, "A communications approach to image steganography," in *Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, vol. 4675, San Jose, CA, USA, January 2002, pp. 26–37.

[60] P. Guillon, T. Furon, and P. Duhamel, "Applied public-key steganography," in *Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, vol. 4675, San Jose, CA, USA, January 2002.

[61] S. Voloshynovskiy, S. P. V. Iquise, and T. Pun, "Towards a second generation benchmark," *Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking*, vol. 81, pp. 1177–1214, June 2001.

[62] S. Voloshynovskiy and T. Pun, "Capacity-security analysis of data hiding technologies," in *IEEE International Conference on Multimedia and Expo ICME2002*, Lausanne, Switzerland, August 26-29 2002.