Errasure Codes in Steganography and Watermarking

HP-SEE

High-Performance Computing Infrastructure for South East Europe's Research Communities

H. Kostadinov[1], N. L. Manev[1,2]

[1] *Institute of Mathematics and Informatics*

[2] Higher School of Civil Engineering "Lyuben Karavelov"

The HP-SEE initiative is co-funded by the European Commission under the FP7 Research Infrastructures contract no. 261499

Basic Terms

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

Cover work (object) is used to refer to the digital object that present a media product: a song, picture, video, or a specific copy of them;

Media is used to refer to the means of representing, transmitting, and recording cover works;

Watermarking is a practice of imperceptibly altering a cover work to embed a message about that work. The goal of watermarking is to prevent piracy or to prove the ownership.

*The term **watermark** is used with two different meanings: the **reference pattern** added to a cover work, and the **message embedded** by that pattern. The right meaning is cleared by the context.*

Application of Watermarking

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

Broadcast monitoring: Identifying when and where works are broadcast by recognizing watermarks embedded in them.

Owner identification: Embedding the identity of a work's copyright holder as a watermark.

Proof of ownership: Using watermarks to provide evidence in ownership disputes.

Transaction tracking: Using watermarks to identify people who obtain content legally but illegally redistribute it.

Content authentication: Embedding signature information in content that can be later checked to verify it has not been tampered with.

Copy control: Using watermarks to tell recording equipment what content may not be recorded.

Steganography

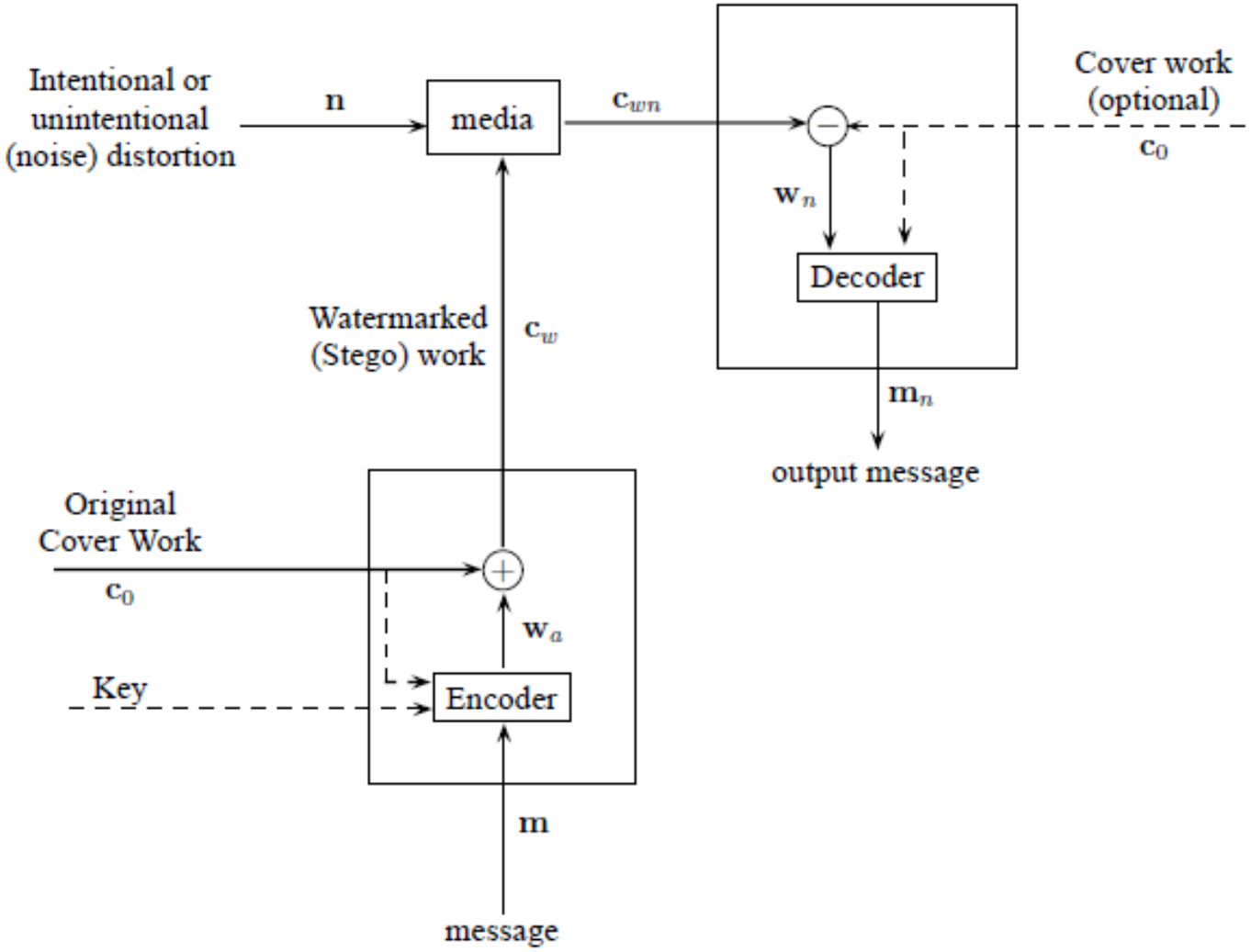
HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

In many practical situations we do not need to provide strong security against removing or modification of the hidden message but it is very important to conceal its existence.

Staganography is the tool that assure this desired undetectable communications between partners. It is a techniques of altering the cover object in undetectable manner, that is, no one but the intended recipient to be able to detect this altering.

The developers of steganograpic techniques assume that their algorithm is known when they analyze their technique but avoid to announce it. Successful steganography is not detectable, so many of the most successful applications may never become public.

The Block Diagram



Required Properties of Watermarking

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

- **Imperceptibility** - The watermark is imperceptible if a normal human being is unable to distinguish (optically or acoustically) the original from the watermarked work.
- **Robustness** refers to the ability to detect the watermark after common signal processing operations like spatial filtering, lossy compression, printing and scanning, and geometric distortions (rotation, translation, scaling, and so on). Robustness does not include intentional attacks based on the knowledge of the algorithms or on availability of the detector functions.
- **Security of a watermark** refers to its ability to resist hostile attacks, such as unauthorized removal, embedding (forgery), and detection. In many watermarking systems, the method by which messages are embedded in cover works depends on a key, and a matching key must be used to detect those marks.

Required Properties for Steganography

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

- **Embedding efficiency**, which is defined as the number of secret message bits embedded per unit distortion.
- **Statistical undetectability** is the probability of detecting a stego work based on the assumed distributions of cover and stego works.
- **Security** refers to the situation in which the warden is active or malicious, rather than passive.

Where to Embed?

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

Watermarks can be embedded by adding to cover works either in spatial domain, or in frequency domain.

- **Spatial domain** is the term used for the standard form of a digital object that represents the media product. For example, a gray-scale image is represented by a matrix whose entries are integers in [0, 255]. Watermarks are embedded by either altering the least significant bit (LSB) or adding a proper noisy pattern.

- **Frequency domain** is the term used for the object obtained after applying to the cover work discrete cosine, discrete Fourier, Hadamard, wavelet, or such other transformations.
  The message is embedded by altering the components of that transformed object, and then applying the reverse transformation.

The Goal of the Talk

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

- This talk presents a part of our research on the use of the error-control codes, mainly in erasure mode, to achieve the goals of watermarking and steganography.
- We have developed an algorithm for embedding in spatial domain that exploits erasure capability of error-control codes. This increases the payload and robustness of watermarking. A lot of experiments have been done with this algorithm.

Error Control Codes

HP-SEE
High-Performance Computing Infrastructure
South East Europe's Research Communities

Let $\mathbb{F} = GF(q)$. Any linear subspace C of dimension k of $\mathbb{F}^n$ is called a ***linear*** $[n, k]$ ***code***.

The ***Hamming weight*** of $\mathbf{v} \in \mathbb{F}$ is $\mathrm{wt}(\mathbf{v}) \stackrel{\text{def}}{=} |\{i \mid v_i \neq 0\}|$.

The ***Hamming distance*** between $\mathbf{u}$ and $\mathbf{v}$ is

$$d(\mathbf{u}, \mathbf{v}) \stackrel{\text{def}}{=} \mathrm{wt}(\mathbf{u} - \mathbf{v}) = |\{i \mid u_i \neq v_i\}|.$$

The smallest distance, $d(C)$, between two codewords of C is called ***minimum distance*** of the code.

A linear code of block length n, dimension k, and minimum distance d is refereed to as $[n, k, d]$ code.

Let a codeword $\mathbf{c} \in C$ is sent trough the channel. The received vector $\mathbf{v}$ can be considered as

$$\mathbf{v} = \mathbf{c} + \mathbf{e}.$$

If $\mathbf{e}$ is a nonzero vector with $\mathrm{wt}(\mathbf{e}) = w$ we say that w ***errors are occurred***.

Erasure Capability

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

Error control codes are used for detecting or correcting errors, or/and for correcting *erasures*. A position of the received vector $\mathbf{v}$, which is expected to be erroneously detected is referred to as an ***erasure***.

Proposition

Let C be a code over a finite field $\mathbb{F}$. The code C can simultaneously correct t errors and s erasures if and only if it has minimum distance $d(C) \geq 2t + s + 1$.

Hence, if the code is used only for correcting erasures it can restore the right values in up to $d(C) - 1$ positions.

The Algorithm - Embedding

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

A-1. Let C be a binary $[n, k]$ linear code. Encode the source message into a binary sequence $\mathbf{m}$.

A-2. Starting with a given state (used as password) of the random number generator generate r reference patterns of size $a \times b$: $\mathbf{W} = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_r\}$.

A-3. Divide (in some way) the cover work into N blocks, $\mathbf{c}_1, \ldots, \mathbf{c}_N$, each of size $a \times b$.

A-4. (optional) Replace the set $\mathbf{W}$ by the set of patterns $\{\mathbf{h}_i\}$ which are orthogonal to all blocks $\mathbf{c}_1, \ldots, \mathbf{c}_N$.

The Algorithm - Embedding

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

A-5. In each block $\mathbf{c}_j$, $j = 1, 2, \ldots, N$, embed r bits of the message sequence $\mathbf{m}$ by

$$\mathbf{c}_{jw} = \mathbf{c}_j + \frac{\alpha}{\sqrt{r}} \left(\epsilon_1 \mathbf{w}_1 + \epsilon_2 \mathbf{w}_2 + \cdots + \epsilon_r \mathbf{w}_r \right),$$

where $\epsilon_i = \begin{cases} 1, & m_{ji} = 1 \\ -1, & m_{ji} = 0 \end{cases}$.

The scale constant α_j controls the tradeoff between visibility and robustness of the watermark.

Then make up the watermarked work gathering back all (now watermarked) blocks. The number of embedded information bits is $\frac{Nrk}{n}$.

The Algorithm – Detection and Decoding

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

A-6. The recipient divides the received image into N blocks $\{\tilde{\mathbf{c}}_j\}$ and knowing the reference patterns (or the key to generate them) calculate

$$\delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i),\ j = 1, 2, \ldots, N,\ i = 1, \ldots, r,$$

where $\delta(,)$ is the chosen detection measure. (Indeed $\tilde{\mathbf{c}}_j$ are noise versions of $\mathbf{c}_{jw}$) Then recover the message:

$$\tilde{\mathbf{m}}_{ji} = \begin{cases} 1, & \text{if} \quad \delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) > \tau \\ 0, & \text{if} \quad \delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) < -\tau \\ \text{an erasure} & \text{if} \quad -\tau \leq \delta(\tilde{\mathbf{c}}_j, \mathbf{w}_i) \leq \tau \end{cases},$$

The Algorithm – Detection and Decoding

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

A-7. The error control code decoder corrects errors and erasures. Its output can be

- "there is no watermarking or hidden message", when the number of erasures is $> N/2$;
- a decoded message (a sequence of bits);
- a decoded message with warning "errors are possible".

Detection Measures

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

The majority of watermarking systems proposed in the literature fall into the class of ***correlation-based watermarking systems***.

Linear correlation:

$$lc(\mathbf{x},\mathbf{y}) = \frac{1}{N}\mathbf{x}\cdot\mathbf{y} = \frac{1}{N}\sum_{i=1}^{N} x_i y_i.$$

Normalized correlation:

$$nc(\mathbf{x},\mathbf{y}) = \frac{\mathbf{x}\cdot\mathbf{y}}{|\mathbf{x}|\cdot|\mathbf{y}|} = \frac{\sum_{i=1}^{N} x_i y_i}{\sqrt{\sum_{i=1}^{N} x_i^2}\sqrt{\sum_{i=1}^{N} y_i^2}}.$$

Correlation coefficient:

$$cc(\mathbf{x},\mathbf{y}) = \frac{\hat{\mathbf{x}}\cdot\hat{\mathbf{y}}}{|\hat{\mathbf{x}}|\cdot|\hat{\mathbf{y}}|} = \frac{\sum_{i=1}^{N} \hat{x}_i \hat{y}_i}{\sqrt{\sum_{i=1}^{N} \hat{x}_i^2}\sqrt{\sum_{i=1}^{N} \hat{y}_i^2}},$$

where $\hat{\mathbf{x}} = \mathbf{x} - E[\mathbf{x}]$ and $\hat{\mathbf{y}} = \mathbf{y} - E[\mathbf{y}]$.

The Case of Normalize Correlation

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

In this case we recommend the following embedding to be used:

A-5

$$\mathbf{c}_{jw} = \mathbf{c}_j \cos\varphi + \epsilon \frac{|\mathbf{c}_j|}{|\mathbf{h}_i|} \mathbf{h}_i \sin\varphi, \qquad (1)$$

where $\epsilon = +1$ or -1, when the embedded bit m_i is 1 or 0, respectively. The parameter φ controls the tradeoff between visibility and robustness of the watermark.

Since $\mathbf{c}_j$ and $\mathbf{h}_i$ are orthogonal and $|\mathbf{c}_{jw}| = |\mathbf{c}_j|$

$$nc(\mathbf{c}_{jw}, \mathbf{h}_i) = \frac{\epsilon |\mathbf{c}_j||\mathbf{h}_i| \sin\varphi}{|\mathbf{c}_{jw}||\mathbf{h}_i|} = \epsilon \sin\varphi.$$

Reconstruction of densities

HP-SEE

puting Infrastructure
Research Communities

Each of the watermark patterns $\mathbf{w}_j$ is obtained by generating an $a \times b$ matrix of real values that are normal gaussian distributed or uniformly distributed on [0,1). Then the matrix is transform into a matrix with zero mean and variance 1. At the end we permute several times rows and columns of the matrix

In our experiments good results are observed with watermarks which are a Kronecker product of matrices with uniformly and gaussian distributed entries.

All above operations depend only on the used pseudo-random generator. Hence, the described procedure can be repeated many times giving the same patterns as the output if each time the initial state of generator is one and the same. Therefore this state can be used as a password.

Error Analysis

HP-SEE

ormance Computing Infrastructure
ast Europe's Research Communities

The expected value of $\delta(,)$ is $\mu_1 = \mu = \frac{\alpha}{\sqrt{r}}$ and $\mu_0 = -\mu = -\frac{\alpha}{\sqrt{r}}$ when $m_i = 1$ and $m_i = 0$ is embedded, respectively (see A-5 and A-6). Let us assume that $\delta(,)$ is normal distributed. Then the variance is $\sigma^2 = \sigma^2_{\boldsymbol{w}_i}(\sigma^2_{\boldsymbol{c}} + \sigma^2_{\boldsymbol{n}})$, where $\sigma^2_{\boldsymbol{w}_{ri}} = 1$, and $\sigma^2_{\boldsymbol{c}}$ and $\sigma^2_{\boldsymbol{n}}$ are the variance the cover work and the channel noise, respectively. Usually $\sigma^2_{\boldsymbol{c}} \approx (60/255)^2$. Let p_c, p_{er} and p_{es} be the probability of correct detection, of error, and of an erasure, respectively. Then in both cases, when $m_i = 1$ and $m_i = 0$ is embedded:

$$p_c = \frac{1}{2}\operatorname{erfc}\left(\frac{\tau - \mu}{\sigma\sqrt{2}}\right); \qquad p_{er} = \frac{1}{2}\operatorname{erfc}\left(\frac{\tau + \mu}{\sigma\sqrt{2}}\right);$$

$$p_{es} = 1 - p_c - p_{er} = \frac{1}{2}\left[\operatorname{erf}\left(\frac{\tau - \mu}{\sigma\sqrt{2}}\right) + \operatorname{erf}\left(\frac{\tau + \mu}{\sigma\sqrt{2}}\right)\right].$$

Error Analysis – the case when no watermark is embedded

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

The probability for an error decision that a given watermark pattern $\mathbf{w}_i$ is embedded (**false positive** error) is

$$p = \operatorname{erfc}\left(\frac{\tau}{\sigma\sqrt{2}}\right) \qquad (\text{since} \quad \mu = 0)$$

The detector will output message if less than $N/2$ erasures are detected. Hence, the **probability for a false positive decision** is given by

$$P_{fp} = \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{i} p^{N-i}(1-p)^i. \qquad (2)$$

Error Analysis – the case when no watermark is embedded

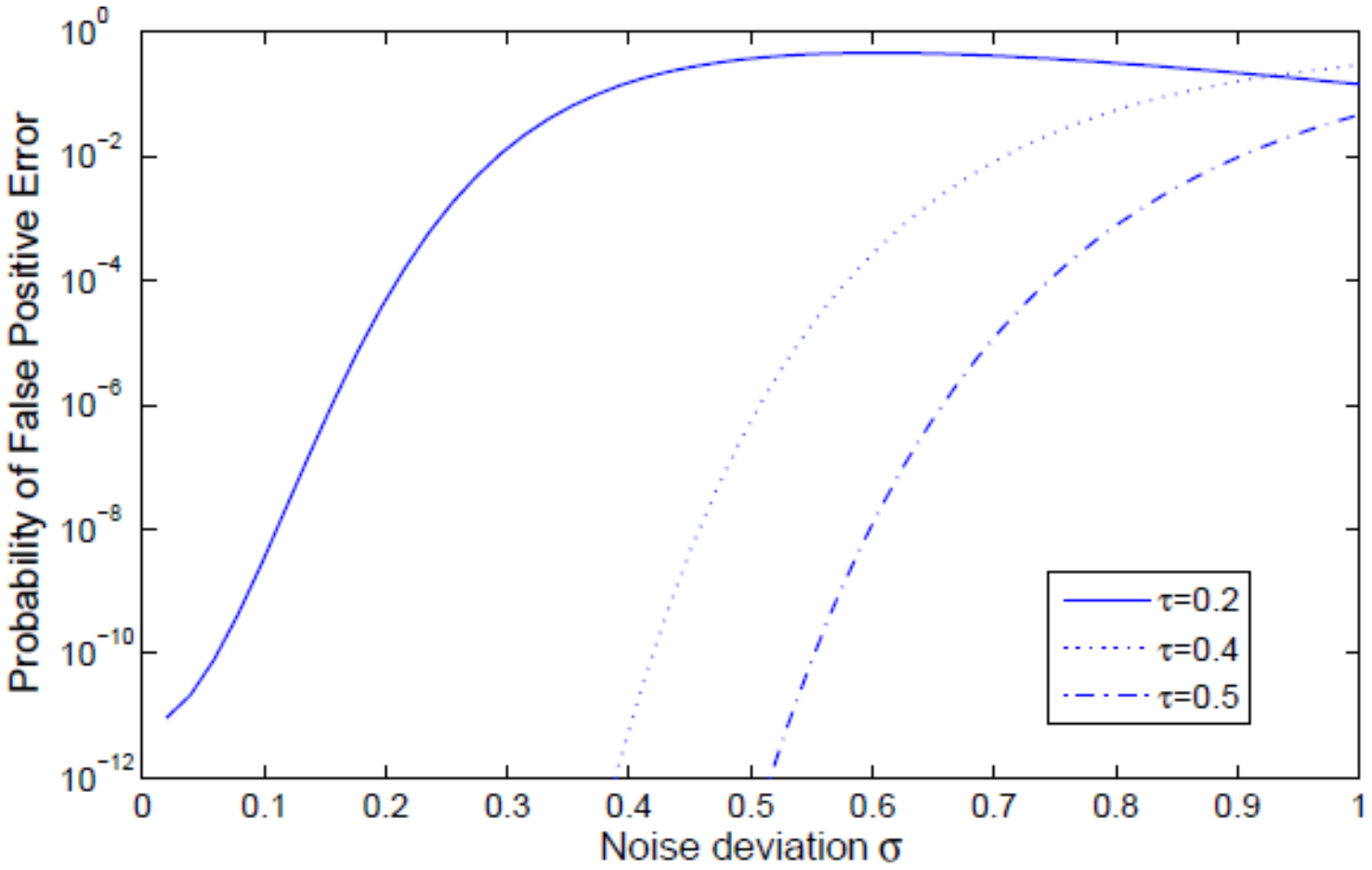


Figure: False Positive Error for $N = 13.16 = 208$ blocks

Error Analysis – the case when a watermark is embedded

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

(a) The embedded n bits can be correctly decoded with a probability

$$P_{corr} = P_1 + P_2 + P_3, \qquad \text{where}$$

$$P_1 = \sum_{s=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{s} p_{es}^{s} \left(\sum_{t=0}^{\lfloor \frac{d-1-s}{2} \rfloor} \binom{n-s}{t} p_{er}^{t} p_{c}^{n-t-s} \right),$$

$$P_2 = \sum_{s=\lfloor \frac{d-1-s}{2} \rfloor + 1}^{d-1} \binom{n}{s} p_c^{n-s} p_{es}^{s}, \qquad P_3 = \sum_{s=d}^{n} \binom{n}{s} p_c^{n-s} (q - p_c)^{s},$$

where d is the minimum distance of the code and $q = \frac{1}{2} \operatorname{erfc}\left(\frac{-\mu}{\sigma\sqrt{2}} \right)$ (this is p_c with $\tau = 0$) is the probability of positive (resp. negative) value of $\delta(\tilde{\mathbf{c}}_{wn}, \mathbf{w}_i)$.

Error Analysis – the case when a watermark is embedded

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

(**b**) The probability of correct decoding in the case when the codes are used only in error correcting mode is given by

$$Q_{corr} = \sum_{t=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{t} q^{n-t}(1-q)^t.$$

(**c**) If more than $N/2$ erasures are marked for a given watermark pattern $\mathbf{w}_i$ then the detector outputs "there is no watermark", that is, it makes **false negative decision**. The probability, P_{fn}, for such an output is given by

$$P_{fn} = \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{i} p_{es}^{N-i}(1-p_{es})^i. \qquad (3)$$

An Example: [13, 8, 4] code

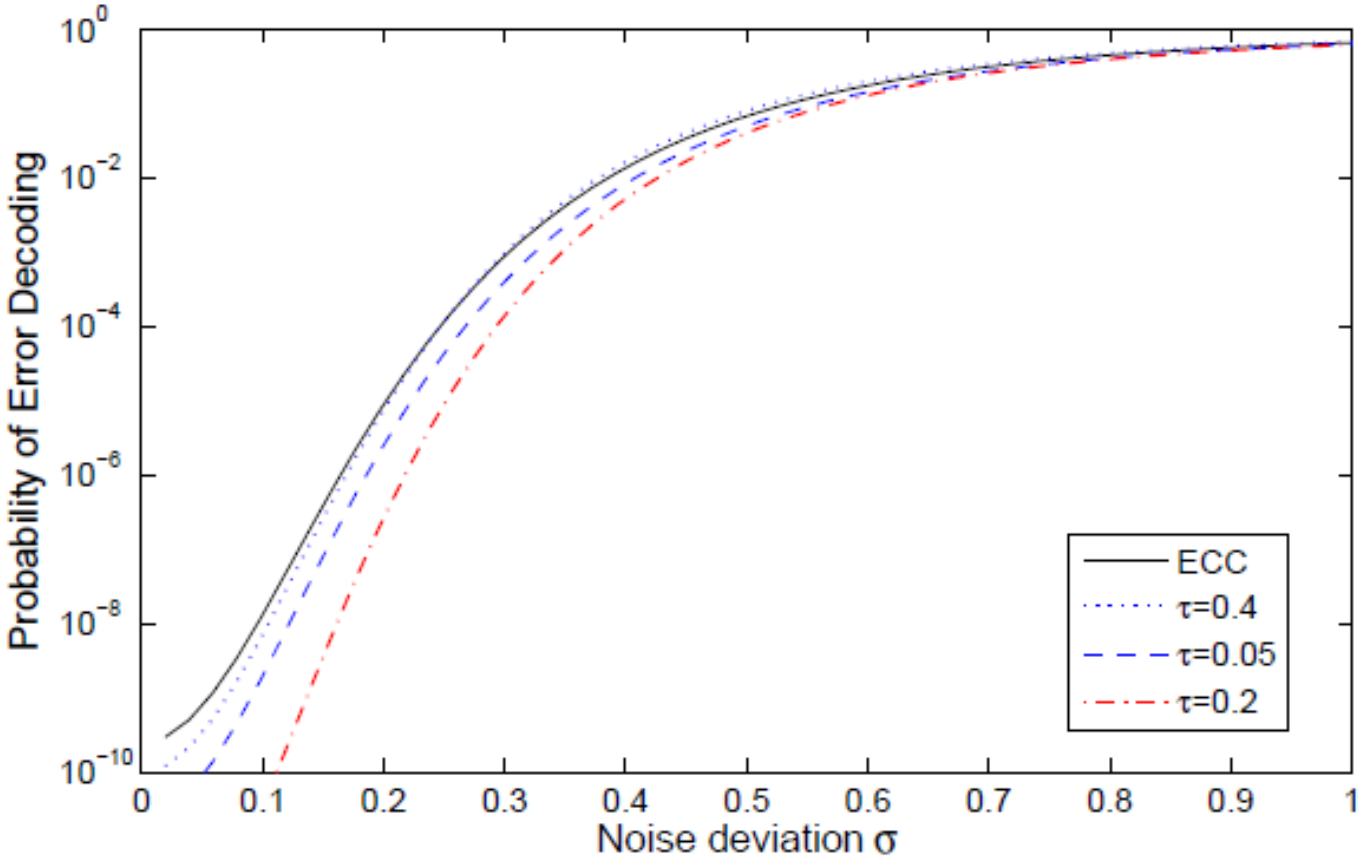


Figure: The probability of error decoding: $1 - P_{corr}$.

Conclusion

HP-SEE
High-Performance Computing Infrastructure for South East Europe's Research Communities

The contribution of our research include:

- *A modified method of embedding that enlarges the payload of watermarking.*
- *A new method of embedding in the case of normalized correlation.*
- *The use of error control codes in erasure mode. This significantly increases the payload and robustness.*