aviesan
alliance nationale
pour les sciences de la vie et de la santé

Institut Thématique Multi-Organismes
Technologies pour la santé

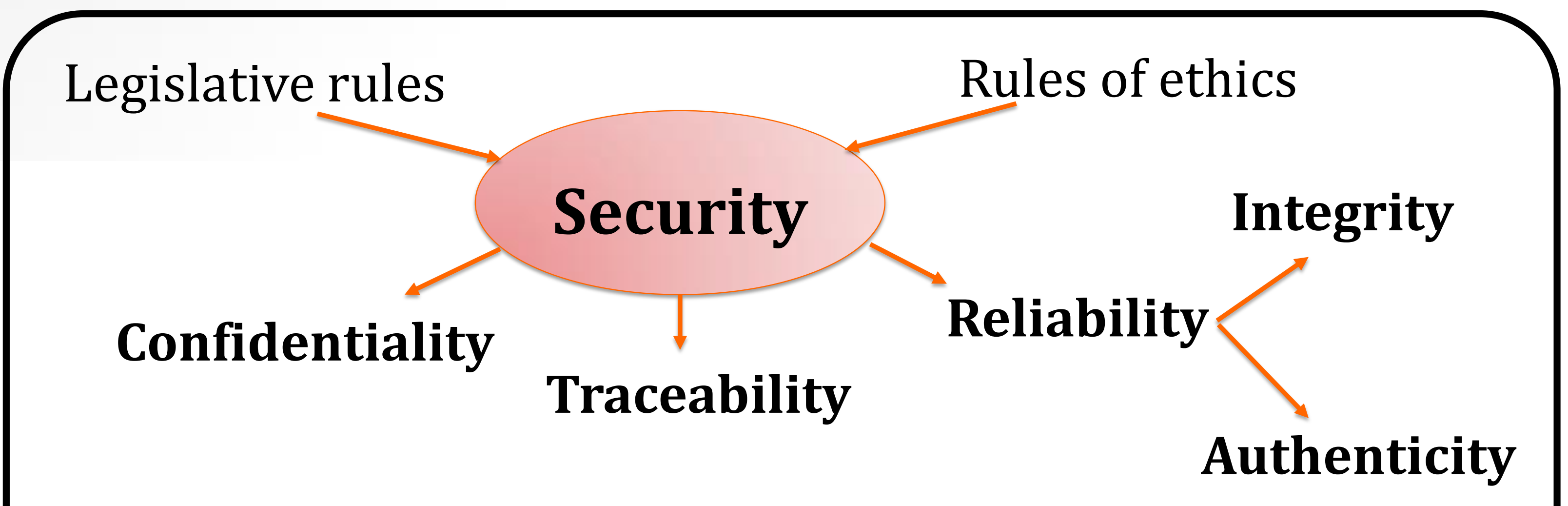
A New Joint Watermarking-Encryption-JPEG-LS Compression Method For A Priori & A Posteriori Image Protection

Sahar HADDAD[1,2], Gouenou COATRIEUX[1,2] , Michel COZIC[3]

1. IMT Atlantique Bretagne-Pays de la Loire 2. LATIM INSERM U1101, Brest 29238, France 3. MEDECOM, Plougastel-Daoulas 29470, France

Objectives/Solution/Results: Trace medical images and verify their integrity or authenticity directly from the compressed bitstream.// The proposed scheme allows message insertion into the image, during the JPEG-LS encoding. // This scheme grants message extraction from the compressed bitstream.// Achieved capacities can provide different watermarking based security services.

1. Issues



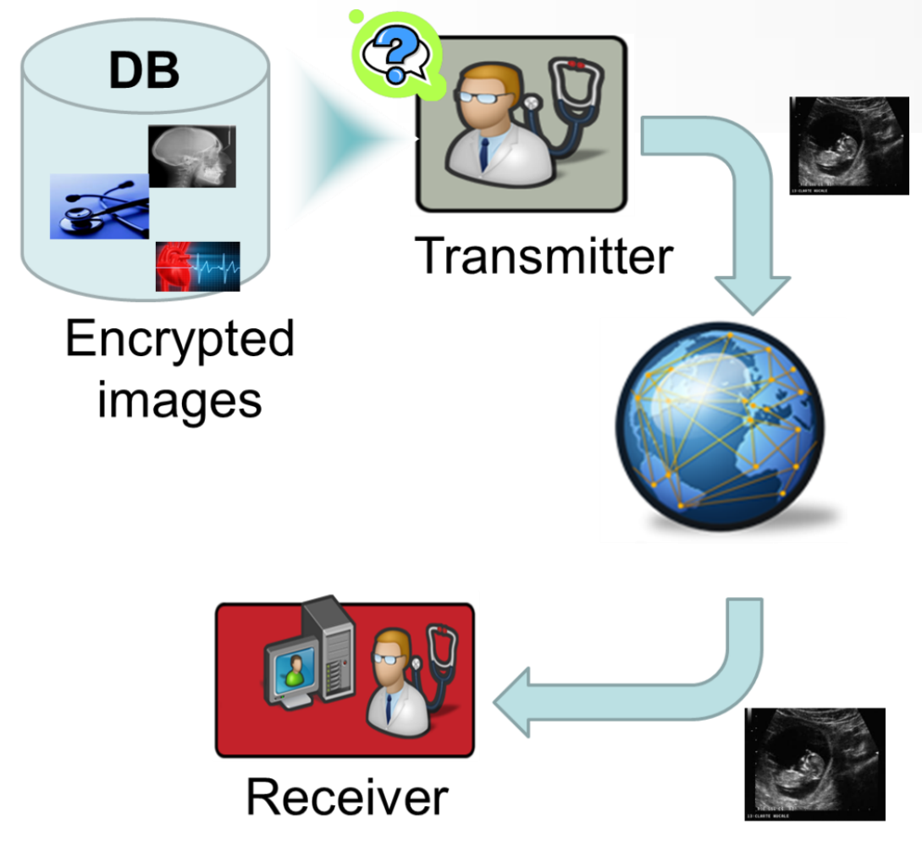
⇨ Objective: Merging encryption (*a priori* protection) and watermarking (*a posteriori* protection*)* into a single security mechanism.

Constraints

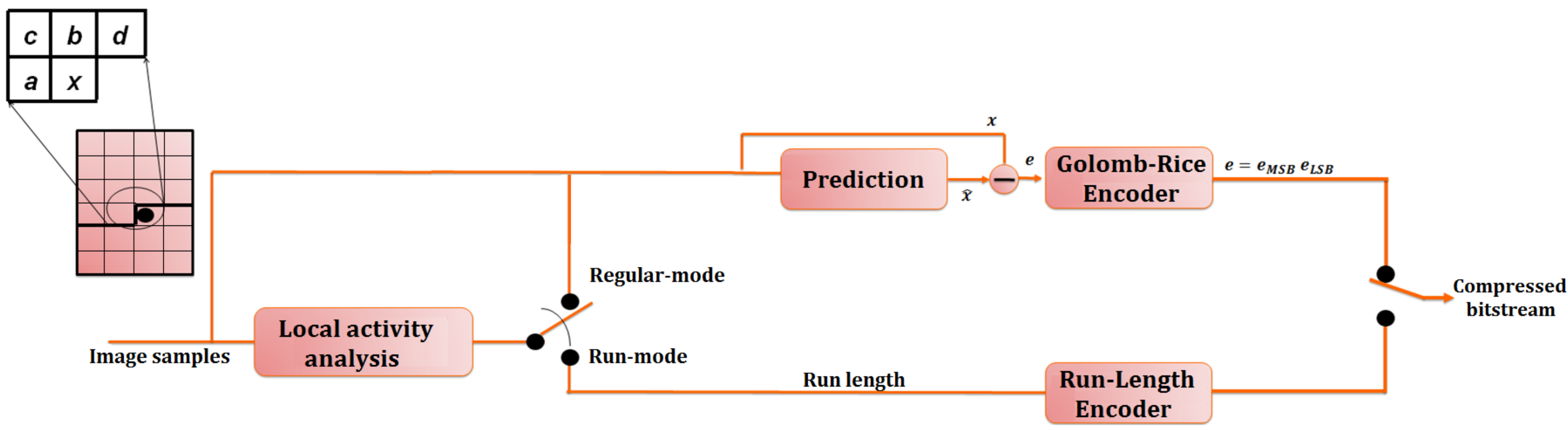
- Healthcare domain induces large volumes of medical images to protect.
- Needs for watermarking-based security services in both compressed and encrypted domains.

⇨ **Watermark extraction directly from the compressed or/and the encrypted image bitstreams.**

⇨ **Interest for joint watermarking, encryption and compression.**



2. JPEG-LS Compression



-General scheme of Lossless JPEG-LS compression-

- $\boldsymbol{x}$: current encoding pixel of an image ; $\{a, b, c, d\}$ the causal neighborhood of x.
- Based on the causal neighborhood of x, JPEG-LS works in 2 modes:

1) Run-mode (if $\boldsymbol{a = b = c = d}$) : Run length encoding (Encoding of the repetition number).

2) Regular-mode**:**

   i) Prediction of x based on the values of $\{a, b, c\}$ ➔ Prediction error: $e = x - \hat{x}$.

   ii) Golomb-Rice encoding of the prediction-error e using the context-dependent factor k :

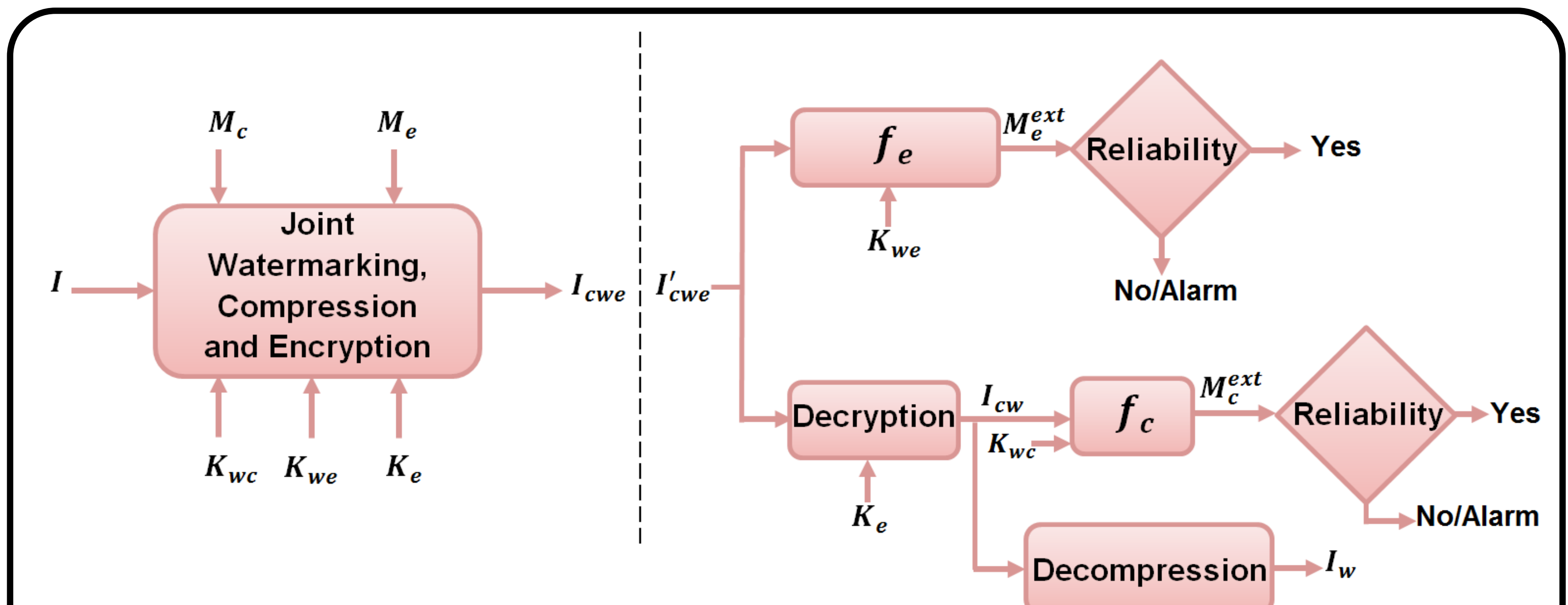
$$\boldsymbol{e = {}'e_{MSB}\ e_{LSB}{}'}$$

Unary code of $\lfloor e/2^k \rfloor$

$\boldsymbol{e_{MSB}} = {}'\,0X1'$; X : sequence of '0's

Binary code of $(e/2^k)$ reminder represented on $\boldsymbol{k}$ bits

3. Joint Watermarking-Encryption-JPEG-LS Compression (JWEC)



-General architecture of the proposed JWEC system-

- I: original image,
- I_{cwe} : watermarked-encrypted-compressed image,
- I_{cw} : decrypted-watermarked-compressed image,
- I_w : decompressed-decrypted-watermarked image,
- K_{wc} and K_{we} are the watermarking keys used in the compressed and encrypted domains, respectively,
- M_c and M_e: messages embedded in compressed and encrypted domains, *resp.*
- M_c^{ext} and M_e^{ext}: messages extracted from compressed and encrypted domains, *resp*.

Compressed bitstream protection & verification

$\boldsymbol{e} = {}'\boldsymbol{e_{MSB}\ e_{LSB}}{}'$: Golomb-Rice coding of the prediction-error.

- If $\boldsymbol{e_{MSB}} = {}'\,0X1'$ (reference sequence) ➔ $\boldsymbol{e^H{}_{LSB} = b_i}$; ($b_i$: i^{th} bit of the message $\boldsymbol{M_c}$; $\boldsymbol{e^H{}_{LSB}}$ higher order bit of e_{LSB}).
- To extract $\boldsymbol{M_c}$, the watermark reader just identifies the reference sequence $'0X1'$ in the compressed bitstream and reads the immediate following bit.
- Example - reference sequence $'0X1' = '\,0001'$ - watermarked-compressed bitstream : ′0000101001**0001**011101**0001**1000001111**0001**111**0001**1010011**0001**001′

➔ The embedded message M_c corresponds to $'01110'$.

Encrypted-compressed bitstream protection & verification

- Encryption based on AES in CBC mode ➔ Compliant with the DICOM standard.
- In the block B_{ci}^{w} (i^{th} block of consecutive bits of the previous watermarked-compressed JPEG-LS bitstream), one bit of $\boldsymbol{M}_{\mathrm{e}}$ is embedded such that:

$$f_e(B_{ci}^{we}, K_{we}) = f_e(AES(B_{ci}^{w}, K_e), K_{we}) = M_{ei}$$

where, f_e is the watermark extraction function in the encrypted domain, K_e is the AES-encryption key and K_{we} is the watermarking key.

4. Experimental results

❖ **Image test set:** 1200 8-bit Retina images and over 700 16-bit X-ray images.

❖ **Performance criteria**

- Image distortion measure between the original image I and its watermarked decompressed-decrypted counterpart I_{wd}

➔Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM).

- Capacity rate in *bpp* (bits of message per image pixel).

Original image

Watermarked image

- Obtained **PSNR** values are greater than 46 dB and 95 dB for retina and X-ray images, *resp.*
- Resulting **SSIM** values are close to 1.
- **Achieved capacities in the encrypted domain:** 0.03 bpp and 0.05 bpp for retina and X-ray images, respectively.
- **Achieved capacities in the compressed domain:** 0.14 bpp and 0.18 bpp for retina and X-ray images, respectively.

5. Conclusion and future works

❖ The proposed joint watermarking-encryption-JPEG-LS scheme allows the access to watermarking-based security services directly from both encrypted and compressed domains.

❖ The proposed scheme guarantees an a priori as well as a posteriori image protection.

❖ The visual quality of the watermarked image is closed to its original version.

❖ Future works will focus on improving the robustness of the watermark to attacks (e.g. lossy image compression, additive noise,…), while preserving the image quality.