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, France
[2] INSERM UMR 1101 LaTIM, Brest 29238, France
[3] MEDECOM, Plougastel Daoulas 29470, France

ABSTRACT

In this paper, we propose the first joint watermarking-encryption-compression scheme for the protection of medical images. Its originality is twofold. In a first time, it allows the access to watermarking-based security services from the encrypted and the compressed bitstreams without having to parse them even partially. It becomes possible to trace images and control their reliability (i.e. integrity and authenticity) from both the encrypted and compressed domains. In a second, it stands on the combination of bit-substitution watermarking, JPEG-LS and the AES block cipher in its CBC mode so as to make our scheme compliant with DICOM. Experiments conducted on different medical images modalities (radiographic and retina images) demonstrate the capability of our system to securely make available a message in both encrypted and compressed domains while minimizing the distortion of the image.

Index Terms— compression, encryption, joint watermarking-encryption-compression, JPEG-LS, security, watermarking.

1. INTRODUCTION

Advances in medical imaging and communication technologies make images play a significant role in diagnosis and patient following. Images are communicated in telemedicine applications (e.g. tele-diagnosis, tele-surgery) as well as mutualized and shared in data warehouses or in the cloud where they can be reused in order to better understand diseases and to develop diagnosis aid support systems [1]. However, such a data access, manipulation and communication over unsecure public networks like Internet increases security needs in terms of data confidentiality, reliability and traceability [2]. Reliability of a piece of information is based on the outcomes of its integrity and authenticity (i.e. proofs that it is issued from the correct source and that it belongs to the correct patient). This is why organizations focus on implementing stringent policies and procedures, based on various security mechanisms. Among these security mechanisms, one can find two complementary mechanisms: encryption and watermarking. Encryption offers an "*a priori*" protection [3] in the sense that, once decrypted, a piece of data is no longer protected. On its side, watermarking [4] provides an "*a posteriori*" protection. Basically, in the case of an image, watermarking embeds or dissimulates into it a message (a set of a security attributes) by imperceptibly modifying its pixel gray values. Depending on the message content, different watermarking-based security services such as integrity control, traceability and usage control can be deployed [5]. As defined, watermarking allows users to access data while maintaining them protected by an invisible watermark. Based on their complementarity in terms of protection there is an interest to combine encryption and watermarking in order to simultaneously ensure an *a priori/ a posteriori* protection [6-7]. We will then refer to crypto-watermarking the main purpose of which is to provide watermarking-based security services from encrypted data [8].

The deployment of such crypto-watermarking protection in medical imaging needs to take into account the specificities of this domain. In particular, medical images represent large volume of data (one hospital generates more than 27,000 terabytes/ year [9]). As a consequence, images are stored in a compressed form so as to reduce costs of storage or of communication. It is thus desirable to develop *a priori*/ *a posteriori* protection solutions that take into account the fact that medical images are compressed.

Most solutions combine watermarking or encryption with compression. One will find methods that conduct encryption with compression jointly [10], i.e. at the same time, or sequentially, i.e. encryption after or before compression [11-12]. Similar solutions have been proposed to provide watermarking-based security services from compressed data [13-15]. Approaches that combine encryption, watermarking and compression are very few [16-17]. They usually independently cascade these three operations. As a consequence, watermarking-based security services are only available in a single domain (spatial or compressed or encrypted).

In this paper, we propose the first joint watermarking-encryption-compression (JWEC) scheme. If it merges these three operations in a single process the decryption, decompression as well as message extraction processes are conducted independently as usually. A first originality of the solution we propose is that it allows the insertion of two messages: one message readable from the encrypted bitstream and the other from the compressed bitstream without having, in both cases, to parse the bitstream, even partially. Second, this scheme combines bit-substitution watermarking with JPEG-LS [18] and the AES block cipher algorithm in its Cipher Block Chaining [19] mode. By doing so, this scheme is compliant with Digital Imaging and Communications in Medicine (DICOM), the medical image standard [20]. This solution makes possible to trace images and control their reliability directly from both encrypted and compressed bitstreams.

The rest of this paper is organized as follows. In section 2, we briefly present JPEG-LS and AES. We then expose the basic principles of our JWEC approach and explain how to combine JPEG-LS and AES with bit-substitution watermarking in Section 3. Some experimental results are provided and discussed in Section 4. Conclusions are drawn in Section 5.

2. AES ENCRYPTION & JPEG-LS IN BRIEF

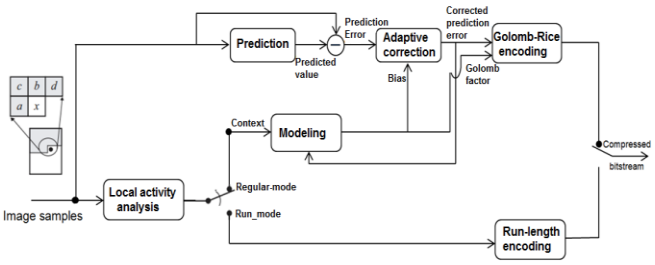

Fig. 1. JPEG-LS compressed bitstream example.

2.1. AES algorithm

The Advanced Encryption Standard (AES) is a symmetric key block cipher exploited in DICOM in its Cipher Block Chaining (CBC) mode. In the CBC mode each block of plaintext, a set of 128 bits, is XORed with the previous encrypted block before being encrypted. As defined, the encrypted version B_i^e of the i^{th} plaintext block B_i is given by:

$$B_i^e = AES(B_i \oplus B_{i-1}^e, K_e) \quad (1)$$

where K_e is the secret AES encryption key.

2.2. JPEG-LS compression

JPEG-LS is a lossless image compression standard supported by DICOM. It relies on the Low Complexity Lossless Compression for Image (LOCO-I) algorithm [21] and encodes pixels depending on a contextual statistical model. The main steps of JPEG-LS are described in Fig. 1. To compress a pixel x, it first analyses its immediate causal neighborhood constituted of previously encoded pixels (pixels *a, b, c* and *d* in Fig. 1) so as to decide in between two encoding modes: regular-mode or run-mode. The decision rule stands on the local gradients:

$$\{g_1 = d - b, g_2 = b - c, g_3 = c - a\} \quad (2)$$

If all the local gradients are null, then the run-mode is activated. Otherwise, the regular-mode is chosen. JPEG-LS run-mode is based on run-length encoding (RLE). It indicates the number of time a gray value is repeated. An inverse unary encoder is used in order to represent the repeated sequence length.

The regular-mode works in a different way. The causal neighborhood of x is used to estimate its gray value $\hat{x}$ with the help of the edge-detecting predictor:

$$\hat{x} = \begin{cases} min(a,b) & if\ c \geq max(a,b) \\ max(a\ b) & if\ c \leq min(a,b) \\ a + b - c & otherwise \end{cases} \quad (3)$$

Because of a prediction bias, a context dependent term $C(Q)$ is computed. This one is derived from the context Q of x. Q is an integer value computed from quantized versions of the local gradients of x, a computation we cannot describe due to paper length limitation. Assuming $C(Q)$ is the bias correction, the corrected prediction error of x is $e_c = e - C(Q)$. Notice that the corrected prediction-error e_c is an integer value.

The last step of the regular-mode consists in Golomb-Rice encoding (GRE) of e_c [22]. GRE encodes a positive integer value p into two parts: the Most Significant Bit part (p_{MSB}) and the Least Significant Bit part (p_{LSB}), that are next concatenated. The MSB-part corresponds to the quotient of the Euclidean division of p by 2^k, where k is the Golomb-Rice factor. This quotient is unary encoded, i.e. by a sequence of '0' ended by '1', the number of '0' being equal to the quotient value. The LSB-part is the binary code of the division reminder encoded on k bits. Notice that The Golomb-Rice factor k of a prediction-error $\tilde{e}$ is context dependent.

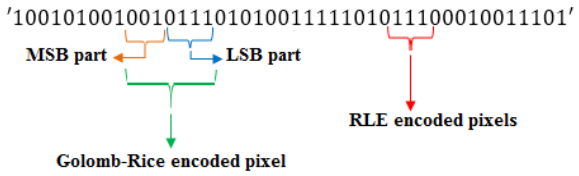

Fig. 2. JPEG-LS compressed bitstream example.

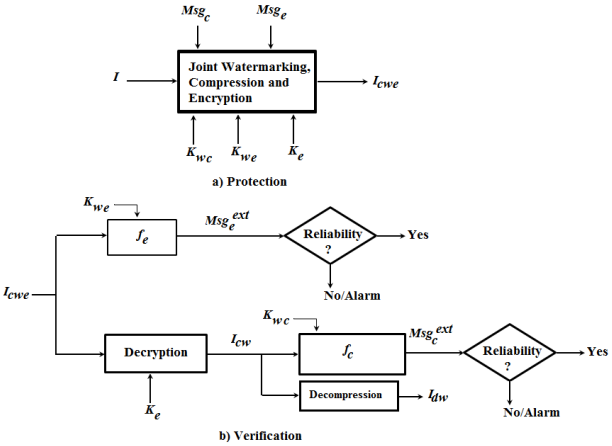

Fig. 3. General architecture of our JWEC system here: $I, I_{cwe}, I_{cw}, I_{dw}, K_{wc}, K_{we}, K_e, Msg_c, Msg_e, Msg_c^{ext}, Msg_e^{ext}$ correspond to the original image, watermarked-encrypted-compressed image, watermarked-compressed image, decompressed-watermarked image, the watermarking keys in compressed and encrypted domains, the encryption key, the embedded and extracted messages from compressed and encrypted domains, respectively.

It varies with the previous encoded prediction-errors of same context.

JPEG-LS decompression works in a similar way. To decode one pixel, the local context is first computed based on the decompressed causal pixel neighborhood to decide which decoding mode to use, i.e. run-mode or regular-mode.

The example given in Fig. 2 illustrates the JPEG-LS encoding of a sequence of pixels. It can be seen that without any additional information it is rather impossible to clearly identify a pixel in the compressed bitstream. There is however a high probability that a sequence '0*X*1'; where *X* is a sequence of '0', indicates the position of a regular-encoded pixel. We will take advantage of this property so as to make a watermarked message available from the compressed bitstream without having to parse it, i.e. without computing any parameters allowing partial image decompression.

3. PROPOSED JOINT WATERMARKING-ENCRYPTION-JPEG-LS COMPRESSION (JWEC) SYSTEM AND SCHEME

In the following, we first present the architecture of the JWEC system we propose for the purpose of verifying the reliability of medical images under their compressed or encrypted forms before explaining how to combine JPEG-LS with bit-substitution watermarking and exposing the whole JWEC scheme.

3.1. System architecture and basic principles

As stated above, the purpose of our JWEC system is to ensure the confidentiality of an image I through encryption while giving access to watermarking-based reliability security services in both

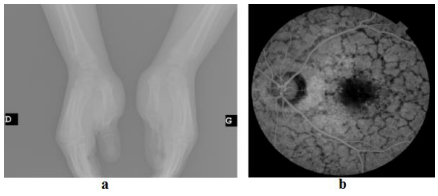

Fig. 4. Image test samples: (a) radiography, (b) retina images

encrypted and compressed domains. As illustrated in Fig. 3, it relies on two main procedures: image protection and image reliability verification.

At the protection stage (see Fig. 3(a)), bit-substitution watermarking, JPEG-LS and AES in its CBC mode are jointly conducted so as to protect *I*. This procedure allows the insertion of two messages, Msg_e and Msg_c that will be readable from the image encrypted bitstream I_{cwe} and from the image compressed bitstream I_{cw}, respectively.

Both messages contain security attributes that assess the image reliability. The embedding and the extraction of each message depend on two watermarking keys: K_{wc} in the compressed domain and K_{we} in the encrypted domain. On its side AES is parameterized with the encryption key K_e.

At the verification stage (Fig. 3(b)), a JWEC protected image I_{cwe} can be decrypted and decompressed in a regular way, that is to say applying AES decryption and JPEG-LS decompression independently. Our JWEC scheme does not need some own decryption and decompression procedures. Watermarking is completely transparent to JPEG-LS and AES. The image reliability can be verified by accessing to Msg_e or Msg_c with the help of two watermarking extraction functions f_c and f_e, respectively.

In the sequel, we first explain how to jointly watermark-JPEG-LS an image before introducing our JWEC scheme.

3.2. JWEC scheme

3.2.1. Compressed bitstream protection (embedding of Msg_c)

As exposed in section 2.2, it is impossible to clearly identify the bits of one pixel in the JPEG-LS-bitstream but there is a high probability that a sequence of bits '$0X1$', where *X* is sequence of '0', corresponds to a pixel encoded in the regular-mode. Hence, we propose to take advantage of this property so as to embed the message Msg_c and to make it readable from the compressed-bitstream without having to parse the compressed bitstream, even partially. To do so, the fundamental of our proposal is to watermark pixels which the Golomb-Rice MSB part of their prediction-errors are encoded such that:

$$\tilde{e}_{MSB} =' 0X1' \quad (4)$$

and to embed one bit of Msg_c in the Golomb-Rice LSB-part encoded on *k* bits.

Moreover, due to the fact that the value of the Golomb factor *k* depends on the pixel context and it is unknown from the watermark reader without parsing the compressed bitstream, we propose to substitute the higher order bit of the Golomb-Rice LSB-part by one bit of the message Msg_c. To make it more clear, let us consider a pixel *p*, the Golomb-Rice factor $k = 4$ and the prediction-error is $\tilde{e} = '00011110'$, where $\tilde{e}_{MSB} = '0001'$ and $\tilde{e}_{LSB} = '1110'$. $\tilde{e}$ will be watermarked into $\tilde{e}_w =' 0001b110' = \tilde{e}_{w-MSB}\,\tilde{e}_{w-LSB}$ where *b* is one bit of the message Msg_c, i.e. $b \in \{0,1\}$. In order to secure the access to Msg_c in the compressed bitstream, we suggest not watermarking all pixels encoded with the reference sequence $\tilde{e}_{MSB} =' 0X1'$. This selection can be made secret based on the watermarking key K_{wc}.

As a consequence and in order to extract Msg_c, the watermark reader has just to identify the reference sequence in the compressed bitstream based on K_{wc} and to read the immediate following bit value.

To be deployed, different constraints have to be considered to guarantee the error-free extraction of Msg_c. For instance, a sequence $\tilde{e}_{MSB} =' 0X1'$ should be followed by an LSB-part $\tilde{e}_{LSB}$ of non-null Golomb-Rice factor *k*. To satisfy this constraint, our system imposes that the Golomb factor *k* of a watermarkable pixel should be equal or greater than 2 so as to give access to a message bit in the compressed domain. On the contrary, that is to say when the MSB-part of the processed pixel prediction error equals $'0X1'$ but its Golomb-factor *k* is smaller than 2, the proposed algorithm shift the prediction error MSB-part to $'X1'$(i.e. $'0X1'$ is changed into $'X1'$).in order to not desynchronize the watermark reader. Some other constraints exist but due to space limitations, we cannot detail them.

In this work, in order to verify the reliability of compressed image, Msg_c is constituted of an authenticity code so as to indicate the image origin and the patient it refers to and a cryptographic hash of the non-watermarked pixels for integrity checking.

3.2.2. Encrypted bitstream protection (embedding of Msg_e)

By definition, the message Msg_e is inserted along with the previous joint watermarking-JPEG-LS. The watermarked compressed bitstream will be modified or watermarked again so as to make Msg_e available from the image watermarked-encrypted-compressed bitstream. One main constraint to consider is that the embedding of Msg_e should not interfere with the one of Msg_c.

Let us consider B_{ci} is the i^{th} block of consecutive bits of the previous watermarked-JPEG-LS compressed bitstream. In the case of AES, such a block is of 128-bit long. Msg_e will be made available in the encrypted domain by modifying B_{ci} into B_{ci}^{w} such that:

$$f_e(B_{ci}^{we}, K_{we}) = f_e(AES(B_{ci}^{w}, K_e), K_{we}) = Msg_e \quad (5)$$

where f_e corresponds to the watermark extraction function in the encrypted domain and K_e is the AES secret key.

In this work, as we are interested in verifying the integrity and authenticity of the encrypted-watermarked-compressed bitstream without having to parse it, we defined the watermarked extraction function f_e as:

$$f_e(B_{ci}^{we}, K_{we}) = SHA(B_{ci}^{we})_j = H_j \quad (6)$$

where H_j corresponds to the j^{th} bit of the cryptographic hash *H* computed with the Secure Hash Algorithm SHA-1. The choice of the value *j* for each AES encrypted-block depends on the secret watermarking key K_{we}. The sequence of bits $\{H_j\}$ corresponds to Msg_e, an authenticity code. In the case encrypted data are tampered, block-hashed will not allowed the corrected recovery of Msg_e, indicating thus the data cannot be used. We invite the reader to refer to [8] for more details about the performance of such reliability control scheme.

The way a watermarked-compressed JPEG-LS block B_{ci} is modified into its version B_{ci}^{w} so as to give access to H_j in the encrypted domain (i.e. $H_j = SHA(B_{ci}^{we})_j$), works in a similar way as the embedding of Msg_c into the JPEG-LS compressed bitstream. It is however an iterative procedure that modifies the prediction errors contained in B_{ci} until H_j is embedded, i.e. so as to verify (6). Let us assume B_{ci} is constituted of *N* Golomb-Rice encoded prediction-errors or equivalently

that $B_{ci} = \{(\tilde{e}_{MSB}, \tilde{e}_{LSB})_u\}_{u=1..N}$. The procedure we propose to insert H_j is the following one:

$u = N$;
$B_{ci}^{w} = B_{ci}$
while $SHA(B_{ci}^{we})_j \neq H_j$
If $\tilde{e}_{MSB,u} \neq' 0X1'$
$bit\_change(\tilde{e}_{LSB,u})$;
$reencode(B_{ci}^{w})$;
$B_{ci}^{we} = AES(B_{ci}^{w}, K_e)$
End if
$u = u - 1$;
End while

where the function $bit\_change()$ modifies one bit of the prediction-error LSB-part ($\tilde{e}_{LSB,u}$), and $reencode()$ corresponds to the function that JPEG-LS re-encodes the modified 128-bit block.

This procedure thus modifies bits of some prediction-errors LSB-parts until H_j is inserted. Because the SHA-1 "strength" is of 80 bits, if 1 bit of B_{ci} changes, then there is one-in-two chance that H_j commutes. As it can be seen, this procedure guarantees that the embedding of Msg_e does not interfere with the one of Msg_c. Beyond, it is important to notice that the embedding of Msg_e induces several other constraints. Indeed, modifying the value of one bit (or equivalently of one pixel) impacts the encoding of the following pixels (see *reencode* function in the above procedure). There is a risk that a compressed pixel changed of plaint-text block (i.e. from B_{ci} to $B_{c(i+1)}$). This may also interfere with the encoding of the next bits of Msg_c. As a consequence, the embedding of Msg_e and of Msg_c have to be considered together during the JPEG-LS compression of the image. More clearly, it is not possible to conduct independently the embedding of Msg_e after the joint watermarking-JPEG-LS compression of the image.

3.3. Image reliability control with JWEC

Our JWCE proposes watermarking-based security services which are transparent to non-compliant watermarking systems. More clearly, any DICOM systems will be able to decipher and decompress a JWEC protected image using AES and JPEG-LS in a regular fashion. On their side, watermarking compliant systems will verify the reliability of images being capable extracting proofs of their integrity and authenticity from both encrypted and compressed domains based on the knowledge of the corresponding watermarking keys, i.e. K_{we} and K_{wc}, respectively.

To extract Msg_e, the encrypted-watermarked-compressed bitstream is first decomposed into blocks of 128 bits, then the extraction function f_e (i.e. in Eq. (6)) is applied to each block. The extracted message is then compared to the image authentication code so as to verify its authenticity and integrity at the same time. In the compressed domain, i.e. after the bitstream decryption using the AES-key K_e, the watermark reader will extract one bit of Msg_c each time reference sequence $'0X1'$ is encountered. The reliability of the image will be verified using the embedded cryptographic hash and authentication code (see Section 3.2.1).

4. EXPERIMENTAL RESULTS

Experiments were conducted on 1200 8-bit encoded retina images of 627x643 pixels and 741 16-bit encoded radiographic images of 1350x1692 pixels. Some samples of our image test set are given in Fig. 5. The following reference sequence $\tilde{e}_{MSB} =' 0X1' = '001'$ is considered for the embedding of Msg_c. All other prediction-errors can be used for the insertion of Msg_e.

The Peak-Signal-to-Noise-Ratio (PSNR) and the structural similarity (SSIM) between the original image I and the decrypted-decompressed-watermarked image I_{wd} (see Fig. 4) are used so as to evaluate the image distortion. Obtained SSIM values are greater than 0.98 for both set of images. These are good values. Obtained PSNR values are greater than 46 dB and 95 dB for our retina and radiographic images test sets, respectively. Compared to a study about lossy JPEG compression for medical images in [23], where it is shown that the diagnosis image value is preserved until the PSNR stays in the range of 40–50 dB, the distortion induced by our JWEC scheme is acceptable. Notice also that the image quality can be better preserved by not watermarking the whole image.

Due to the fact that one bit of the message Msg_e is embedded per AES-block, the watermark capacity in the encrypted domain depends on the image size and depth as well as on the JWEC compression rate. Based on our image test sets, the achieved capacities in the encrypted domain, expressed in bits of message per pixel of image (bpp), are of 0.03 bpp and 0.05 bpp for retina and radiographic images respectively. Regarding the capacity in the compressed domain, the size of Msg_c depends on the statistical distribution of the reference sequence $'0X1'$. The capacities we obtained are of 0.18 bpp (i.e. a message of about 240537 bits) and of 0.14 bpp for radiographic and retina images, respectively. These capacities are large enough so as to allow various security services ranging from integrity to traceability [8].

In terms of complexity, our JWEC algorithm needs about twice the time necessary for the JPEG-LS compression code, but it gives access to watermarking-based security services in both compressed and encrypted domains.

To the best of our knowledge, in the literature there is no equivalent solution to the scheme we propose. Nevertheless, we propose to compare its performance in terms of distortion to the ones of the schemes presented in [16] and [17]. Both combine compression, watermarking and encryption, in a cascade manner, with watermarking-based services available only in the spatial [16] and encrypted [17] domain. Regarding the capacity/distortion compromise, the method in [16] offers for the well-known reference image "Lena" a maximum capacity of 29748 bits (i.e. 0.1 *bpp*) with a PSNR of 35.22 *dB*, while [17] achieves a capacity of 1980 bits (0.007 *bpp*) with PSNR of 38 *dB*. On its side, our scheme provides PSNR and capacity values of 42.7 *dB* and 52757 bits (i.e. 0.2 *bpp*) in the compressed domain, respectively; thus a much better capacity/distortion compromise compared to [16] and [17].

5. CONCLUSION

In this paper, we have proposed the first joint watermarking-encryption- JPEG-LS compression scheme, the purpose of which is to offer a simultaneous *a priori*/*a posteriori* image protection. It combines bit-substitution watermarking with JPEG-LS and AES in its CBC mode making it fully compliant with DICOM. Our scheme gives access to two messages in the compressed and in the encrypted domains without having to parse the bitstreams even partially. We further demonstrated how these messages can be used for verifying reliability of an image in both domains. Even though this JWEC scheme induces an image information loss, it well preserves the diagnosis value of images. Beyond, offered capacities are large enough so as to allow various watermarking-based security services. Future works will focus on improving the robustness and reducing the complexity of our scheme.

6. REFERENCES

[1] J. Vincent, W. Pan, and G. Coatrieux, "Privacy protection and security in eHealth cloud platform for medical image sharing", In *Advanced Technologies for Signal and Image Processing* (ATSIP), 2016 2nd International Conference on. IEEE, 93–96, 2016.

[2] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, "Relevance of watermarking in medical imaging", In *Information Technology Applications in Biomedicine, Proceedings,* EMBS International Conference on IEEE*,* pp. 250-255, 2000.

[3] R. L. Lagendijk, Z. Erkin and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation", *IEEE Signal Processing Magazine*, 30(1), pp. 82-105, 2013.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*, Morgan Kaufmann, 2007.

[5] W. Pan, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens and C. Roux, "Watermarking to enforce medical image access and usage control policy", in *sixth international conference on signal-image technology and internet-based systems* (SITIS). IEEE, pp. 251–60, 2010.

[6] D. Bouslimi, G. Coatrieux, M. Cozic and C. Roux, "An a priori and a posteriori protection by means of data hiding of encrypted images: application to ultrasound images", In *The International Conference on Health Informatics,* Springer, Italy, pp. 220-223, 2014.

[7] D. Bouslimi, G. Coatrieux, C. Quantin, F. A. Allaërt, M. Cozic and C. Roux, "A teleassistance protocol based on joint watermarking–encryption evidence for identification of liabilities in case of litigation", *IRBM*, 36(5), pp. 279–86, 2015.

[8] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images" *Signal Processing: Image Communication*, *47*, pp. 160-169, 2016.

[9] "What's next for the health-care data center?", http://www.datacenterjournal. com/whats-healthcare-data-center/. Accessed: 06-04-2015.

[10] Q. Wang, M. Wei, X. Chen and Z. Miao, "Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system", *Multimedia Tools and Applications*, pp. 1-20, 2017.

[11] B. M. Shreedhar, I. L. Vishal and N. Hemavathi, "Image Encryption-Then-Compression System via Prediction Error Clustering and lossless encoding", *International Journal of Innovative Research in Information Security*, *4*(2), pp. 33-39, 2015.

[12] H. K. Aujla and R. Sharma, "Designing an Efficient Image Encryption-Then Compression System with Haar and Daubechies Wavelet", *International Journal of Computer Science and Information Technologies*, *5*(6), pp. 7784-7788, 2014.

[13] S. Haddad, G. Coatrieux, M. Cozic and D. Bouslimi, "Joint Watermarking and Lossless JPEG-LS Compression for Medical Image Security", *IRBM*, 38(4), pp. 198-206, 2017.

[14] J. Fridrich, M. Goljan, Q. Chen and V. Pathak, "Lossless data embedding with file size preservation", International Society for Optics and Photonics, Security, Steganography and Watermarking of Multimedia Contents VI, Vol. 5306, pp. 354-366, 2004.

[15] R. Caldelli, F. Filippini and M. Barni, "Joint near-lossless compression and watermarking of still images for authentication and tamper localization", *Signal Processing: Image Communication*, *21*(10), pp. 890-903, 2006.

[16] A. V. Subramanyam, S. Emmanuel and M. S. Kankanhalli, "Compressed-encrypted domain JPEG2000 image watermarking", *IEEE International Conference on Multimedia and Expo (ICME),* pp. 1315-1320, 2010.

[17] Z. Qian, X. Zhang and S. Wang, "Reversible data hiding in encrypted JPEG bitstream", *IEEE transactions on multimedia*, *16*(5), pp. 1486-1491, 2014.

[18] The Joint Photographic Experts Group (JPEG), FCD 14495, "Lossless and near-lossless coding of continuous-tone still image jpeg-ls", *The International Standards Organization (ISO)*/*The International Telegraph and Telephone Consultative Committee* (CCITT), 1997.

[19] S. Frankel, R. Glenn and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", *IETF RFC 3602*, Sept. 2003.

[20] J. M. Silva, G. T. Marques, D. Silva and C. Costa, "Web Validation Service for Ensuring Adherence to the DICOM Standard", *Studies in health technology and informatics*, *235*, pp. 38-42, 2017.

[21] M. J. Weinberger, G. Seroussi and G. Sapiro, "The loco-i lossless image compression algorithm: principles and standardization into jpeg-ls", *IEEE Trans. Image Processing*, 9(8), pp. 1309-24, 2000.

[22] W.D. Leon-Salas, "Encoding compressive sensing measurements with Golomb–Rice codes", IEEE international symposium on circuits and systems (ISCAS), pp. 2177-2180, 2015.

[23] K. Chen, T.V. Ramabadran, "Near-lossless compression of medical images through entropy coded DPCM", *IEEE Transactions on Medical Imaging*, 1994.