



e-ISSN: 2319-8753 | p-ISSN: 2320-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.512

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com



Joint Watermarking for Image Reliability Control in Encrypted and Compressed Domains: A Review

Miss. Ishwari Pund¹, Prof.Chandrakant R Barde²

Master of Engineering, Gokhale Education Society's R. H. Sapat College of Engineering, Management Studies and Research, Nashik, India

Gokhale Education Society's R. H. Sapat College of Engineering, Management Studies and Research, Nashik, India

ABSTRACT: Sharing medical images can enormously help doctor in their day by day practice by permitting them to arrive at a symptomatic all the more rapidly. However, such images are sensitive and should be ensured. In this paper, propose the principal joint watermarking-encryption pressure conspire for the insurance of medicalimages. Its inventiveness is twofold. In a first time, it permits the admittance to watermarking-based security administrations from the scrambled and the compacted bitstreams without parsing them even part of the way. It gets conceivable to follow images and control their dependability from both the encoded and compacted spaces. In a second, it remains on the blend of spot replacement watermarking, JPEG-LS and the AES block figure in its CBC mode to make our plan. Tests directed on various medicalimages modalities (radiographic and retina pictures) show the ability of our framework to safely make accessible a message in both scrambled and compacted areas while limiting the contortion of the images.

KEYWORDS: Joint watermarking-encryption-compression, JPEG-LS, security, watermarking,block cipher.

I. 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 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. 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. Reliability of a piece of information is based on the outcomes of its integrity and authenticity. 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 in the sense that, once decrypted, a piece of data is no longer protected. On its side, watermarking provides an “a posteriori” protection. Basically, in the case of an image, watermarking embeds or dissimulates into it a message 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. 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. We will then refer to crypto-watermarking the main purpose of which is to provide watermarking-based security services from encrypted data.

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. 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, i.e. at the same time, or sequentially, i.e. encryption after or before compression. Similar solutions have been proposed to provide watermarking-based security services from compressed data. Approaches that combine

encryption, watermarking and compression are very few. They usually independently cascade these three operations. As a consequence, watermarking-based security services are only available in a single domain.

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 and the AES block cipher algorithm in its Cipher Block Chaining mode. By doing so, this scheme is compliant with Digital Imaging and Communications in Medicine (DICOM), the medical image standard. This solution makes possible to trace images and control their reliability directly from both encrypted and compressed bitstreams.

Organization of paper

The organization of the paper is as follows section II gives the related work and limitations and last section concludes the paper with future work followed by references.

II. LITERATURE REVIEW

J. Vincent, W. Pan, and G. Coatrieux: In this paper, author propose two methodology to understand this issue. Initial, a reserving outsider that forestall the cloud supplier (CP) to connect the records from their season of procurement is proposed. At that point the utilization of Oblivious Transfer (OT) is advanced to keep the CP from realizing which pictures are gotten to by a given purchaser specialist. The worldwide design for clinical pictures sharing is then portrayed and talked about.

D. Bouslimi and G. Coatrieux: In this paper, author propose a novel crypto-watermarking framework to check the dependability of medical images and following them, for example recognizing the individual at the source of an illicit revelation. This framework couples a typical watermarking strategy, in light of Quantization Index Modulation (QIM), and a joint watermarking-decoding (JWD) approach. At the producer side, it permits the inclusion of a watermark as a proof of unwavering quality of the images before sending it encoded; at the gathering, another watermark, a discernibility evidence, is inserted during the unscrambling cycle. The scheme. author propose makes interoperate these two watermarking approaches considering dangers of impedances between installed watermarks, permitting the admittance to both dependability and detectability confirmations. Exploratory outcomes affirm the proficiency of our framework, and exhibit it very well may be utilized to recognize the root of a divulgence regardless of whether the image has been modified.

J. C. Dagadu and J. Li: In this paper, author propose a security framework for secure transmission of medical images in telemedicine applications. The framework couples an IWT-LSB watermarking and an encryption dependent on arbitrary stage and bedlam, to guarantee secrecy, respectability, verification and nonrepudiation of medical images. author use IWT because of the touchy idea of medical images and the need to hold symptomatic quality after image remaking. Trial results and dissects show that the framework gives adequate protection from different types of assaults.

Z. Qian, X. Zhang, Y. Ren, and G. Feng: This paper expects to introduce an elective technique achievable for block-enciphered images. Before transferring information to a distant worker, the substance proprietor encodes the first image with a square code calculation utilizing an encryption key. At that point, the worker implants extra pieces into the scrambled image with an installing key to create the stamped encoded image. On the beneficiary side, the extra pieces can be extricated if the recipient has the implanting key. In the event that the recipient has just the encryption key, the stamped encoded image can be legitimately interpreted to a plaintext image with great quality. At the point when both the installing and encryption keys are accessible for the collector, he can recuperate the first image with no errors.

C. V. Kumar, V. Natarajan, K. Nirmala, T. Balasubramanian, K. R. Rao, and S. Krishnan: In this paper, a proficient RW strategy is recommended that recoups the installed information from the stamped scrambled shading palette images within the sight of attacks. In this technique, embeddable shading significantly increases are developed by utilizing shading parceling. Next, the cryptographic SHA-256 hash and Bose-Chaudhuri-Hocquenghem (BCH) are applied over the mystery data to guarantee the validness and honesty. The hash verified mystery information is

implanted into the scrambled shading palette image. The mystery information is extricated utilizing the distinct shading parceling strategy and confirmed with cryptographic hash work. The proposed technique has higher inserting limit when contrasted with other relative plans. The BCH codes assists with recouping the mystery information and spread image within the sight of commotion and attacks.

S. Haddad, G. Coatrieux, M. Cozic, and D. Bouslimi: In this paper, creator present another joint watermarking-pressure plot the innovation of which remains in the mix of the lossless pressure standard JPEG-LS with the piece replacement watermarking regulation. This plan permits the admittance to watermarking-based security administrations without decompressing the picture. It gets conceivable to follow pictures or to confirm their realness straightforwardly from their compacted bitstream. Execution of our plan, communicated as far as inserting limit and bending, are assessed on ultrasound pictures. They show that the watermarked pictures don't perceptually contrast from their unique partners while offering a limit sufficiently huge to help different security administrations.

In this paper, author present another joint watermarking-pressure plot the inventiveness of which remains in the mix of the lossless pressure standard JPEG-LS with the spot replacement watermarking adjustment. This plan permits the admittance to watermarking-based security administrations without decompressing the image. It gets conceivable to follow images or to check their validness straightforwardly from their packed bitstream. Execution of our plan, communicated as far as implanting limit and bending, are assessed on ultrasound images. They show that the watermarked image don't perceptually contrast from their unique partners while offering a limit sufficiently huge to help different security administrations.

C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan: Computerized Imaging and Communications in Medicine (DICOM) is one among the critical organizations utilized worldwide for the portrayal of medical images. Without a doubt, medical images security assumes an urgent part in telemedicine applications. Combining encryption and watermarking in medical images insurance prepares for upgrading the confirmation and more secure transmission over open channels. In this unique situation, the current work on DICOM image encryption has utilized a fluffy disordered guide for encryption and the Discrete Wavelet Transform (DWT) for watermarking. The proposed approach conquers the constraint of the Arnold change—one of the most used disarray components in image encoding. Different measurements have validated the adequacy of the proposed medical images encryption calculation.

X.-J. Tong, P. Chen, and M. Zhang: This paper set forward another image lossless pressure joint encryption calculation dependent on tumultuous guide with all unique data flawless. The lossless pressure utilizes SPIHT (Set Partitioning in Hierarchical Trees) encoding technique dependent on number wavelet change, and scramble different rounds during the time spent wavelet coefficients and SPIHT coding applying numerous sorts of turbulent guides. Test results show that the packed document size is around 50 % of the first record size, which accomplishes moderately great lossless pressure proportion. Also, the encryption technique finishes numerous security assessments, for example, affectability test, entropy test, autocorrelation test, NIST SP800–22 test. There is a high application esteem in the medical field and the public security office whose image documents require a moderately high caliber.

H. Ga and W. Zeng: this paper advances the image compression and encryption dependent on the wavelet change and bedlam by consolidating the upsides of disorganized planning. This strategy presents the turmoil and wavelet change into the advanced image encryption calculation, and changes the image from the spatial space to the recurrence area of wavelet change, and adds the cross breed commotion to the high recurrence part of the wavelet change, consequently accomplishing the reason for the image corruption and improving the encryption security by consolidating the encryption approaches in the spatial area and recurrence space dependent on the clamorous succession and the phenomenal qualities of wavelet change. Testing tests show that such calculation lessens the memory utilization and executes the unpredictability, not exclusively can diminish the key investing and pack the energy spending, yet additionally can improve the nature of decoded and reproduced image, subsequently indicating great encryption highlights with better encryption impact.

Z. Qian, H. Xu, X. Luo, and X. Zhang: During information covering up, creator propose a joined inserting calculation including two phases, the Huffman code planning and the arranged histogram moving. The inserting strategy is reversible. At the point when an approved client requires a downloading activity, the worker removes extra messages from the checked encoded JPEG bitstream and recuperates the first scrambled piece stream losslessly. Subsequent to downloading, the client gets the first JPEG bitstream by an immediate decoding. The proposed structure out-performs



past deals with RDH-EI. To start with, since the undertakings of information implanting/extraction and bitstream recuperation are completely cultivated by the worker, the picture proprietor and the approved client are needed to actualize no additional activities aside from JPEG encryption or decoding. Second, the installing payload is bigger than best in class works.

III. OPEN ISSUES

Lot of work has been done in this field because of its extensive usage and applications. In this section, some of the approaches which have been implemented to achieve the same purpose are mentioned. These works are majorly differentiated by the algorithm for joint watermarking system systems.

The purpose of our proposed system is to ensure the confidentiality of an image through encryption while giving access to watermarking-based reliability security services in both encrypted and compressed domains. As illustrated in system architecture, it relies on two main procedures: image protection and image reliability verification.

At the protection stage, bit-substitution watermarking, JPEG-LS and AES in its CBC mode are jointly conducted so as to protect. This procedure allows the insertion of two messages, and that will be readable from the image encrypted bit stream and from the image compressed bit stream, respectively. Both messages contain security attributes that assess the image reliability. The embedding and the extraction of each message depend on two watermarking keys: in the compressed domain and in the encrypted domain. On its side AES is parameterized with the encryption key.

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

IV. 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 bit streams 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.

REFERENCES

- [1] J. Vincent, W. Pan, and G. Coatrieux, "Privacy protection and security in eHealth cloud platform for medical image sharing," in Proc. 2nd Int. Conf. Adv. Technol. Signal Image Process. (ATSIP), Mar. 2016, pp. 93–96.
- [2] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," *Signal Process., Image Commun.*, vol. 47, pp. 160–169, Sep. 2016.
- [3] J. C. Dagadu and J. Li, "Context-based watermarking cum chaotic encryption for medical images in telemedicine applications," *Multimedia Tools Appl.*, vol. 77, no. 18, pp. 24289–24312, Sep. 2018.
- [4] Z. Qian, X. Zhang, Y. Ren, and G. Feng, "Block cipher based separable reversible data hiding in encrypted images," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13749–13763, Nov. 2016.
- [5] C. V. Kumar, V. Natarajan, K. Nirmala, T. Balasubramanian, K. R. Rao, and S. Krishnan, "Encrypted separable reversible watermarking with authentication and error correction," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7005–7027, Mar. 2019.
- [6] S. Haddad, G. Coatrieux, M. Cozic, and D. Bouslimi, "Joint watermarking and lossless JPEG-LS compression for medical image security," *IRBM*, vol. 38, no. 4, pp. 198–206, Aug. 2017.



- [7] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains," *Comput. Methods Programs Biomed.*, vol. 159, pp. 11–21, Jun. 2018.
- [8] X.-J. Tong, P. Chen, and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," *Multimedia Tools Appl.*, vol. 76, no. 12, pp. 13995–14020, Jun. 2017.
- [9] H. Ga and W. Zeng, "Image compression and encryption based on wavelet transform and chaos," *Comput. Opt.*, vol. 43, no. 2, pp. 258–263, Apr. 2019.
- [10] Z. Qian, H. Xu, X. Luo, and X. Zhang, "New framework of reversible data hiding in encrypted JPEG bitstreams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 351–362, Feb. 2019.



INNO  **SPACE**
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details