

A Novel Tamper Detection-Recovery and Watermarking System for Medical Image Authentication and EPR Hiding

Afaf Tareef¹, *IEEE Student Member*, Ahmad Al-Ani², Hung Nguyen², Yuk Ying Chung¹

Abstract— Recently, the literature has witnessed an increasing interest in the study of medical image watermarking and recovery techniques. In this article, a novel image tamper localization and recovery technique for medical image authentication is proposed. The sparse coding of the Electronic Patient Record (EPR) and the reshaped region of Interest (ROI) is embedded in the transform domain of the Region of Non-Interest (RONI). The first part of the sparse coded watermark is used for saving the patient information along with the image, whereas the second part is used for authentication purpose. When the watermarked image is tampered during transmission between hospitals and medical clinics, the embedded sparse coded ROI can be extracted to recover the tampered image. The experimental results demonstrate the efficiency of the proposed technique in terms of tamper correction capability, robustness to attacks, and imperceptibility.

Index Terms— Watermarking, Medical imaging, ROI, Tamper recovery, Sparse coding.

I. INTRODUCTION

With the rapid growth of modern communication technology and biomedical engineering; remote exchange of medical information between hospitals and medical clinics has become faster and easier. During transmission, medical data can be intentionally or unintentionally manipulated which may lead to dangerous consequences. Due to the importance of medical images in many crucial applications related to life of human, such as clinical diagnosis, treatment, and surgery, an integrity verification and tamper detection techniques have become more and more urgent demands.

Image watermarking is one of the earliest technologies for integrity and authenticity of digital content. Recently, the medical image authentication has become one of the main watermarking priorities. Medical image watermarking can be divided into three main categories: data hiding techniques (for hiding electronic patient records) [1,2,3], authentication techniques (including tamper detection and recovery) [4,5,6], and hybrid authentication and data hiding techniques [7,8,9,10]. In the last few years, hybrid authentication and data hiding techniques have received an increasing attention due to its multiple advantages, e.g., EPR hiding, authentication of the ROI, and recovering a tampered region.

Unlike other types of digital multimedia watermarking, medical image watermarking should be implemented in an extra careful manner, as modifying a certain region of the image may lead to misdiagnosis. That region is called the Region of Interest (ROI), i.e., the region that contains the most significant information related to patient's diagnosis and accordingly must be stored without any distortion. In this algorithm, Region of Non-Interest (RONI), which is the rest of the image that does not include ROI, is used as a host part to embed dual watermarks; Electronic patient Record (EPR) and the second watermark is the ROI that will be used in case of tampering the watermarked medical image. Sparse Coding (SC) is applied to encode the EPR and ROI to enable high compression with high reconstruction quality. Singular Value Decomposition (SVD) is applied on the host part due to its stability and resistance to geometric attacks. Embedding in this transformed domain is chosen to make the algorithm more robust and imperceptible.

The rest of paper is organized as follows: Background knowledge is briefly introduced in section II. In section III, the proposed technique is illustrated. Section IV presents the experimental results. Finally, section V gives the conclusion.

II. BACKGROUND

In order to optimize the watermarking characteristics in our technique, Sparse Coding (SC) is applied on the concatenated watermark. SC is an approach to factorize the input vectors into a weighted linear combination of a set of dictionary vectors under sparsity constraints [11]. In other words, each input vector $\vec{\xi} \in R^K$ can be succinctly represented by the following equation:

$$\vec{\xi} \cong \sum_{i=1}^n \vec{b}_i s_i \quad (1)$$

Where $\vec{b}_i \in R^K$ is the i^{th} dictionary vector and $\vec{s} \in R^n$ is the sparse vector. The dictionary is usually over-complete ($n > k$), and thus capture a large number of patterns in input data. Recently, SC has successfully been used in many applications, such as compression, noise reduction, feature extraction, and pattern classification. The main merit of meeting a high level of imperceptibility and robustness in our technique is due to using sparse coding. It enhances the imperceptibility by providing a high compression, so only a few number of nonzero coefficients will be embedded in the host image. These few number of coefficients can efficiently reconstruct the coded signal even when under attacks and this is the reason behind achieving the robustness aspect.

Another powerful tool used in the proposed technique is the Singular Value Decomposing (SVD). SVD is a linear

¹Afaf Tareef and Yuk Ying Chung are with the School of Information Technologies, University of Sydney, NSW 2006, Australia (e-mail: atar8654@usyd.edu.au, vera.chung@sydney.edu.au).

²Ahmad Al-Ani and Hung Nguyen are with Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia (e-mail: ahmed@eng.uts.edu.au, Hung.Nguyen@uts.edu.au).

algebra scheme that decomposes a matrix to three matrices, two unitary matrices and one diagonal matrix. SVD is presented as following:

$$X = U \Sigma V^T \quad (2)$$

Where U and V are the left and right eigenvectors and S is a diagonal matrix with nonnegative real numbers. SVD has many applications, such as image compression and noise reduction. In our technique, singular value matrix is used as a host part because it contains intrinsic algebraic image properties and it is less affected by image processing operations.

III. THE PROPOSED APPROACH

Our proposed watermarking technique can be summarized into three phases: watermark generation phase, embedding phase, and extraction and recovering phase. Assume the size of the host image is $m \times n$ pixels and for the EPR is $r \times c$ pixels. The implementation phases of our proposed technique are summarized in figure 1.

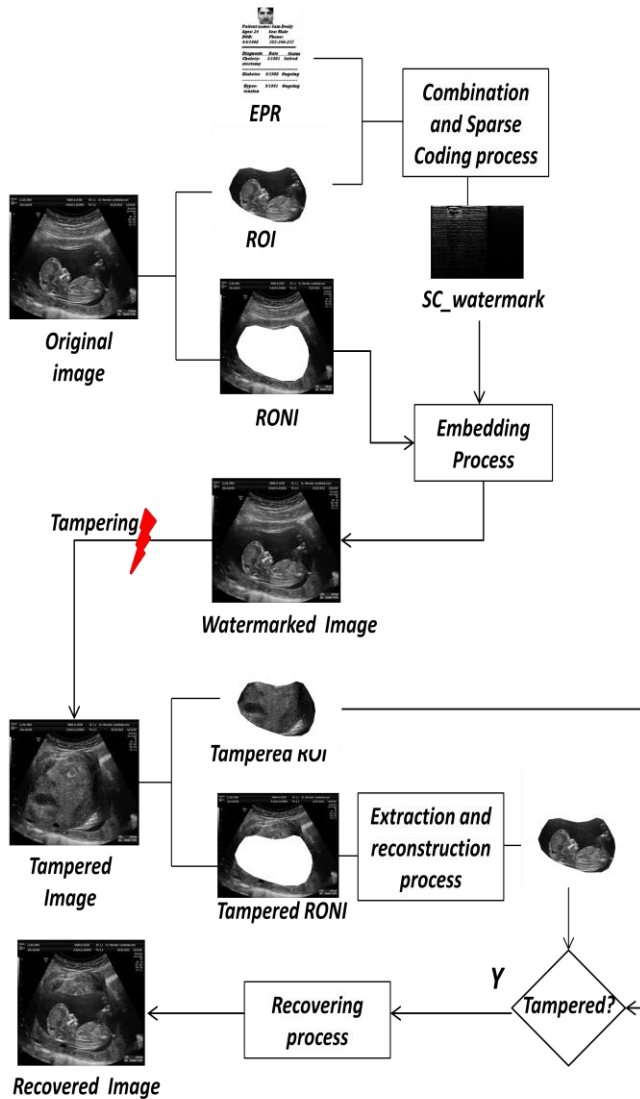


Figure 1. Flowchart of the proposed technique

A. The watermark generation phase

To generate the watermark, the following steps are implemented:

- 1) Separate the host image I into two regions, I_{ROI} and I_{RONI} . In order to accurately separate, the ROI can be taken in any shape, unlike many of existing techniques where the ROI is taken as a square in shape so some parts of ROI may be eradicated or part of the RONI may be included in the square.
- 2) Reshape I_{ROI} to get a rectangle image of r rows. Then, concatenate it with the EPR watermark to get W with $r \times v$ size.
- 3) Sparse encode the watermark to get W_{SC} using over-complete dictionary of size $r \times v$ by solving equation 1 to succinctly encode the watermark in a few number of coefficients. The sparse coding of the EPR and ROI are jointly embedded to meet two different goals; protection of sensitive data and data authentication.

B. The embedding phase

For embedding, follow the detailed steps:

- 1) Reshape I_{RONI} to get matrix with minimum r rows. Let us denote it X_{RONI} . Then apply SVD:
$$X_{RONI} = U \Sigma V^T \quad (3)$$
- 2) Embed the sparse coding of the concatenated watermark W_{SC} into the singular value matrix. \oplus denotes an addition operator and γ is the scaling factor.
$$M\Sigma = \Sigma \oplus \gamma W_{SC} \quad (4)$$
- 3) Apply SVD again on the $M\Sigma$ to get $U_w, V_w,$ and Σ_w .
- 4) Reconstruct the watermarked RONI matrix to get X'_{RONI} . U_w and V_w are the extraction key.
$$X'_{RONI} = U \Sigma_w V^T \quad (5)$$
- 5) Reshape X'_{RONI} and combine it with I_{ROI} to get the watermarked image I' .

C. The extraction and Recovery phase

The extraction phase is described by following:

- 1) Separate the watermarked (maybe tampered) image H to get H_{ROI} and H_{RONI} . Then, reshape H_{RONI} into matrix and apply SVD to get $U', V',$ and Σ'_w .
- 2) Reconstruct the watermarked singular value $M\Sigma'$ using the U_w and V_w to extract the embedded SC by $W'_{SC} = (M\Sigma' \ominus \Sigma'_w) / \gamma$.
- 3) Reconstruct the concatenated watermark by multiplying the extracted W'_{SC} by the dictionary to get W' . Then, separate the watermark to retrieve extracted EPR watermark and reshaped ROI watermark.
- 4) Now tamper detection and recovery takes place, the absolute difference between the extracted ROI watermark and the ROI of the tampered

watermarked image H_{ROI} is used to detect the tampering.

- If tamper is detected, the extracted ROI watermark is replaced with the tampered pixels to get the recovered image.

IV. EXPERIMENTAL RESULTS

The test set consisted of ten Ultrasound (US) images of size 512×512 pixels and 256×256 gray-scale EPR image. For the experiments presented here, over-complete DCT dictionary is used in the sparse approximation T-MSBL [12] technique to represent the concatenated watermark. Figure 2 shows (a) one of the test images and (b) the corresponding watermarked image, and the EPR image is shown in (c). The figure indicates that the quality of our watermarked image is very high.

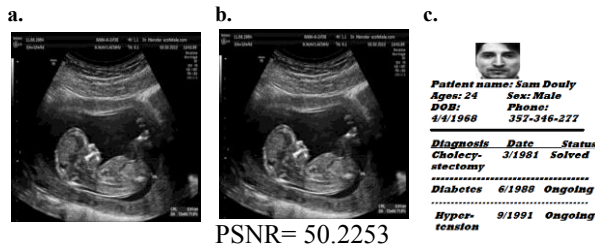


Figure 2. (a) the original image, (b) the watermarked image, (c) EPR

To evaluate the performance of our technique, Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC) are used to evaluate the imperceptibility and robustness, respectively. The high PSNR and NC values are corresponding to great similarity between images. PSNR is defined as:

$$PSNR = 10 \times \log_{10} \frac{255^2 \times M \times N}{\sum_{i=1}^M \sum_{j=1}^N (G(i,j) - G'(i,j))^2} \quad (6)$$

Where G is the original host image, and G' is the watermarked image. M and N the width and height of the original image. To achieve imperceptibility, the PSNR value should be above 30 dB. With our technique using 0.05 threshold, the PSNR values for the ten test images are between (47-53) dB with average 49.8169 dB, which indicates a high level of imperceptibility. To evaluate the quality of extracted watermark, NC between the original and recovered watermark is calculated using the following equations.

$$NC = \frac{\sum_i \sum_j W \times W'}{\sqrt{\sum_i \sum_j W^2 \times \sum_i \sum_j W'^2}} \quad (7)$$

W and W' are the original and extracted watermark, respectively. To demonstrate the robustness and tamper detection and recovery, several kinds of attack and tamper are applied on the watermarked image, as discussed in the following three subsections.

A. Performance under Image operations

In this section, four types of very strong image distortion are applied to the watermarked image (i.e., Blurring, Gaussian noise addition (variance= 0.5), Hard threshold, and JPEG

compression (quantity factor=2)). Figure 3 shows the tampered images with their PSNR values, the extracted EPR with the NC values, and the corresponding recovered images using the extracted ROI. According to the results in figure 3, the robustness of our technique is met with high fidelity from serious corrupted images where the PSNR values for all attacked images are less than 25 dB. The NC between the extracted EPR and ROI watermarks and the original ones are always greater than 0.80 and 0.86, respectively, which indicates to a high level of robustness.

Attacked Image	Extracted EPR	Recovered image
Blurring (PSNR=22.8529)	NC= 0.9343	NC= 0.9938
Gaussian Noise (PSNR=7.6222)	NC= 0.8043	NC= 0.8637
Hard threshold (PSNR=15.2264)	NC= 0.9575	NC= 0.9855
JPEG compression (PSNR=24.8584)	NC= 0.9542	NC= 0.9979

Figure 3. Results after image operations

B. Performance under addition attacks

In this section, the watermarked image is modified by adding objects of different sizes and in different locations. The results are shown in figure 4. The embedded EPR and ROI can be successfully extracted from the tampered images.

C. Performance under cropping and removal attacks

In figure 5, some content removal and cropping attacks are applied to the watermarked images, such as removing the ROI and cropping half of image. It is clear that our technique

has a good ability to recover the tampered ROI even if the tampered area is large outperforming of other existing techniques which deal with small tampered area. The NC values between the original and extracted EPR and ROI are always above 0.95.







Attacked Image	Extracted EPR	Recovered image
 PSNR=17.3843	 Patient name: Sam Douly Age: 24 Sex: Male DOB: 4/8/1968 Phone: 357-346-277 Diagnosis Date Status Cholecyst 3/1981 Solved stectomy Diabetes 6/1988 Ongoing Hypertension 9/1991 Ongoing	 NC=0.9951
 PSNR=22.6943	 Patient name: Sam Douly Age: 24 Sex: Male DOB: 4/8/1968 Phone: 357-346-277 Diagnosis Date Status Cholecyst 3/1981 Solved stectomy Diabetes 6/1988 Ongoing Hypertension 9/1991 Ongoing	 NC=0.9964

Figure 4. Results after addition attacks







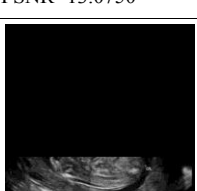


Attacked Image	Extracted EPR	Recovered image
 PSNR=22.7157	 Patient name: Sam Douly Age: 24 Sex: Male DOB: 4/8/1968 Phone: 357-346-277 Diagnosis Date Status Cholecyst 3/1981 Solved stectomy Diabetes 6/1988 Ongoing Hypertension 9/1991 Ongoing	 NC=0.9982
 PSNR=13.0750	 Patient name: Sam Douly Age: 24 Sex: Male DOB: 4/8/1968 Phone: 357-346-277 Diagnosis Date Status Cholecyst 3/1981 Solved stectomy Diabetes 6/1988 Ongoing Hypertension 9/1991 Ongoing	 NC=0.9980
 PSNR=14.4250	 Patient name: Sam Douly Age: 24 Sex: Male DOB: 4/8/1968 Phone: 357-346-277 Diagnosis Date Status Cholecyst 3/1981 Solved stectomy Diabetes 6/1988 Ongoing Hypertension 9/1991 Ongoing	 NC=0.9948

Figure 5. Results after removal attacks

The experimental results prove that the embedded watermark can survive in image processing operations such as, Blurring, Gaussian Noise, Hard threshold and JPEG compression, and in addition and removal attacks. The experiments demonstrate the ability of our proposed method to successfully reconstruct the ROI and EPR even when tampering a large area of the watermarked image.

V. CONCLUSION

In this paper, a novel medical image watermarking and tamper localization and recovery technique is proposed to verify the integrity and authenticity of the medical content. The proposed technique can be used for multiple purposes; EPR hiding, authentication of the ROI, and recovering a tampered region. The experimental results demonstrate that our technique not only offer a good tamper correction rate but also a high robustness and perceptual quality of the watermarked image. The main merit of the efficiency of our technique is due to combining sparse coding and SVD techniques. We believe that this work will find a good practical medical applications.

REFERENCES

- [1] D. Anand and U. C. Niranjana, "Watermarking medical images with patient information." In *Engineering in Medicine and Biology Society, Proceedings of the 20th Annual International Conference of the IEEE*, pp. 703-706. 1998.
- [2] J. Nayak, P. S. Bhat, M. S. Kumar, and U. R. Acharya, "Reliable transmission and storage of medical images with patient information using error control codes," in *proceedings of the First India Annual Conference, IEEE INDICON*, pp. 147-150. 2004.
- [3] Pan, Wei, et al. "An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform." *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*. IEEE, 2010.
- [4] Zain, Jasni M., and Abdul RM Fauzi. "Medical image watermarking with tamper detection and recovery." *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*. IEEE, 2006.
- [5] Huang, Hui, et al. "Medical image integrity control and forensics based on watermarking—Approximating local modifications and identifying global image alterations." *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*. IEEE, 2011.
- [6] Hisham, Syifak Izhar, et al. "Digital watermarking for recovering attack areas of medical images using spiral numbering." *Electronics, Computer and Computation (ICECCO), 2013 International Conference on*. IEEE, 2013.
- [7] Zain, Jasni M., L. P. Baldwin, and M. Clarke. "Reversible watermarking for authentication of DICOM images." *Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE*. Vol. 2. IEEE, 2004.
- [8] Al-Qershi, Osamah M., and Bee Ee Khoo. "ROI-based tamper detection and recovery for medical images using reversible watermarking technique." *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*. IEEE, 2010.
- [9] O. M. Al-Qershi, B. E. Khoo. "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images". *Journal of digital imaging* 24.1, pp. 114-125. 2011.
- [10] Das, Sudeb, and Malay Kumar Kundu. "Effective management of medical information through ROI-lossless fragile image watermarking technique." *Computer methods and programs in biomedicine* 111. pp.662-675.2013.
- [11] Lee, Honglak, et al. "Efficient sparse coding algorithms." *Advances in neural information processing systems* 19, 801,2007.
- [12] Z. Zhang, D. R. Bhaskar, "Sparse signal recovery with temporally correlated source vectors using sparse Bayesian learning." *Selected Topics in Signal Processing, IEEE Journal of* 5.5, pp. 912-926. 2011.