Robust Blind Medical Image Watermarking Using Quantization and SIFT with Enhanced Security

Tuan Nguyen-Thanh and Thuong Le-Tien
Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City, Vietnam
Vietnam National University Ho Chi Minh City (VNU-HCM), Ho Chi Minh City, Vietnam
Email: {nttuan, thuongle}@hcmut.edu.vn

***Abstract*—The paper proposes an efficient blind robust watermarking solution for medical images based on a combination of the Scale Invariant Feature Transform (SIFT) and even-odd quantization. Unlike most existing methods using SIFT with original image, our proposed algorithm can extract the embedded information without original image by selecting only non-overlapping features in embedding process and exploiting the correlation among all detecting regions. As a result, both detection and extraction of embedded information can be obtained with our method. Moreover, it can be expanded to multi-bit watermarking with two suggestions of fan-shaped and half-ring-shaped regions. The experimental results are implemented with various medical images and evaluated about the quality, the reliability and the robustness against common medical image processing attacks including filtering, compression, rotation, scaling and cropping. Furthermore, the security in embedding and extracting information is also enhanced in our solution.**

***Index Terms*—SIFT, quantization-based watermarking, blind medical image watermarking**

I. Introduction

In the early 1990s, watermarking began to gain attention and rapidly developed in many areas such as copyright protection, copy control, monitoring, secure communication, data integration, authentication, and verification, etc. Recently, the boom in demand for transmission and storage the medical images over Internet to support telemedicine as well as smart healthcare promotes the extensive research of watermarking techniques for different medical images. This expansion opens many opportunities and challenges to meet the specific requirements of the medical industry such as the privacy, confidentiality, security, reliability, standards, and applications [1]-[5].

In general, watermarking is the technique of embedding and extracting the information (or watermark) in host data (also known as cover data). Although watermarking can be applied to various types of cover data, image watermarking has always received great attention in theoretical researches as well as practical applications. The data after embedding is called watermarked data (or embedded data). This data can be altered by attacks in the form of normal data processing or intentional damage, which is called attacked data. This data is used to extract the embedded information. Thus, like the background of information theory, a general watermarking system can be considered with three main components: embedder, attack channel and extractor.

Based on the need of the original data in the extraction process, watermarking system is classified into blind and non-blind. The first model is more applied in practical because of extracted information from embedded data without the cover data. However, blind watermarking systems must face to more challenges to obtain high performance.

Considered generally, there are three main requirements in a typical watermarking system: transparency, robustness, and capacity. Transparency requirement evaluates the perceptibility or quality degradation of the embedded data with the cover data. Robustness requirement considers the ability of extracting information against attacks. Capacity requirements mentions the amount of the embedded information. In fact, there is always a trade-off between these requirements. Therefore, for fair evaluation and comparison, it is necessary to ensure that the methods used for the survey are tested under the same conditions.

In order to evaluate the embedded image quality, subjective assessment through visual perception and objective evaluation through quantitative parameters can be used. In fact, subjective assessment of image quality is very difficult because it depends a lot on the observer as well as the observed image, so it is not possible to use tools to automatically evaluate image quality. Objective quantities commonly used are the Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR) or the Normalized Cross Correlation coefficient (NCC). However, there is absolutely no clear relationship between these quantities and Human Visual System (HVS). A recently proposed solution to measure image fidelity is the Structural SIMilarity index (SSIM) related to structural information in image blocks by measuring the similarity in luminance, contrast, and structure.

Manuscript received May 30, 2021; revised November 26, 2021.

doi: 10.12720/jait.13.1.45-52

Depending on the application, there are different requirements for embedded capacity. Generally, watermarking can be classified into single bit and multiple bits. One-bit watermarking is suitable to detect whether a given image is embedded information or not, while multi-bit watermarking is used for extracting the content of embedded information. Note that in some watermarking methods, in addition to affecting the quality of the embedded image, the amount of embedded information also depends on the size and characteristics of the embedded image.

Attacks in image watermarking can be classified into non-synchronization and synchronization [6]. Attacks in the first type only change the certain values of image pixels but remain whole their positions. They include noise, filtering, compression, etc. On the contrary, the latter attacks change the certain positions of image pixels, thus they are also called as geometrical attacks. Especially, they are called pure synchronization attacks if they remain their values, such as cropping, flipping, translation, rotation with a multiple of 90 degrees, etc. In other cases, they change both values and positions of image pixels, such as scaling, rotation with not a multiple of 90-degree, etc.

Based on common image watermarking, various watermarking algorithms have been extended for medical images [7]-[13]. In general, many existing studies on watermarking for medical imaging have been only applied to a certain type of medical image without considering the specific requirements related to the medical field such as reliability and security. Some of them need the original image or the embedded features in extraction process. This limits the range of applications in practice. Moreover, these methods have not fully considered attacks, including both non-synchronization and synchronization. Therefore, based on analyzing and evaluating existing solutions, the paper focuses on offering some effective solutions to meet the following objectives:

1) Allowing to extract information without the original image.
2) Successfully extracted information against many different types of attacks, both non-synchronization (filtering, compression) and synchronization (rotation, scaling, cropping).
3) Can be applied to common medical images, while ensuring reliability and security requirements in the medical field.

II. Related Works

A. Spread Spectrum-Based Watermarking

Cox *et al.* [14] were the first to exploit spread spectrum communication theory to construct watermarking algorithms. It requires the original image at the first time. Other authors also use the concept of spread spectrum but in a different way that does not require the original data during extracting process. The basic idea of this approach is to add a watermark pattern generated from a pseudo-random number generator through a secret key. The watermark is extracted using a correlation detector with the same embedded key. This means that only the correct key used during embedding can extract the exact information that was embedded in the original image. Thus, security is greatly increased compared to other techniques. Due to spreading the watermark over the entire image, this method also achieves imperceptibility and robustness. On the other hand, since there is no need for original data, spread-spectrum based watermarking is suitable for many applications. In addition, the spread-spectrum technique used in watermarking can be performed directly in the spatial domain or other transform domains such as DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), etc. However, the embedded signal itself is considered noise, so it can cause significant errors in the extraction process. Therefore, several improved spread spectrum methods have been studied to partially overcome the limitations of traditional spread spectrum [15], [16].

Because the extraction process using the correlation detector requires synchronization of the size and position between the watermark and the attacked image, the spread spectrum-based watermarking technique is less robust against most synchronization attacks. Moreover, only one bit of information is embedded in this technique.

B. Quantization-Based Watermarking

Unlike spread spectrum-based watermarking techniques using a watermark pattern corresponding to a region of image for each information bit, embedding and extracting information in quantization-based watermarking is implemented at local value pixels [17]. In this approach, one information bit is embedded and extracted directly by one image pixel. It is less robust to non-synchronization attacks than spread spectrum-based watermarking because a significantly change in even only one embedded pixel also causes the failure of information extraction process. However, it can be survived to synchronization attacks by determining the position of the embedded information based robust features. In order to improve the robustness in the case there is a slight loss of synchronization, the information bit can be embedded repeatedly in a patch around the features.

The quantization index $Q(x,y)$ corresponding to each embedded pixel is calculated by:

$$Q(x,y) = \begin{cases} 0, if\ k \le \frac{I(x,y)}{\Delta} < (k+1)\ with\ k\ even \\ 1, if\ k \le \frac{I(x,y)}{\Delta} < (k+1)\ with\ k\ \ odd \end{cases} \quad (1)$$

Then, the quantization error is calculated by:

$$r(x,y) = I(x,y) - \Delta.floor(\frac{I(x,y)}{\Delta}) \quad (2)$$

Based on the quantization index, the quantization error and the embedded bit *w*, the watermarked image is implemented as follows:

$$I'(x,y) = I(x,y) + u(x,y) \quad (3)$$

where $u(x,y) =$

$$\begin{cases} -r(x,y) + 0.5\Delta, if\ Q(x,y) = w; \\ -r(x,y) + 1.5\Delta, if\ Q(x,y) \ne w\ and\ r(x,y) > 0.5\Delta; \\ -r(x,y) - 0.5\Delta, if\ Q(x,y) \ne w\ and\ r(x,y) \le 0.5\Delta. \end{cases} \quad (4)$$

In addition to subjective criteria, the original image and embedded image are compared based on objective criteria such as the distortion *D* or the peak signal to noise ratio *PSNR*:

$$D = || I'(x,y) - I(x,y) ||^2 \quad (5)$$

$$PSNR = 10log_{10}\frac{255^2}{D} \quad (6)$$

Another metric to measure the quality of the embedded image is the Structural Similarity index (*SSIM*):

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (7)$$

where μ_x , μ_y , ${\sigma_x}^2, {\sigma_y}^2$, σ_{xy} are the mean, variance, covariance of x and y correspondingly; $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are two variables for stabilization. In this paper, we set $k_1 = k_2 = 0.05$ and $L = 255$.

The extracted bit is determined as the same result with the quantization index corresponding to the attacked pixel.

With a larger quantization width Δ, the higher the ability to extract accurate information because the larger distance between the quantization levels in the two sets makes it easy to distinguish two values of information bit "0" and "1", but in return the quality of the quantized image will decline significantly because the quantized value changes significantly compared to the original value. In the special case Δ=1, even-odd quantization becomes the Least Significant Bit (LSB) technique. This is the first studies on image watermarking by embedding the watermark as a binary random sequence into the remaining LSB of the image after 7-bit grayscale histogram compression and uses a bit comparator to detect watermark [18], [19]. Some other authors perform embedded binary information directly in the LSB planes of the image. This approach is simple and obtains high capacity with good quality. However, since the information can be retrieved if the embedding location is determined, the security of this method is very low. In addition, a small change in the embedded image can cause inaccurate extracted information. In other words, it is only suitable for secure error-free channel applications.

Moreover, the same information bit can be embedded into multiple features so that the information bit is still extracted successfully in the case of disappearance of several embedded features in attacked image. In this case, the decision of final extracted information is based on the larger number of extracted bits 0s and 1s.

Obviously, when extracting information from the value corresponding to the actual embedding location, it will give the correct result while it will give a random result either bit 0 or 1 for the non-embedding value. Consequently, if there is loss of synchronization even with only one pixel, the extracted bit can be inaccurate. To improve the robustness due to this loss of synchronization by attacks, the same information bit can be embedded into an area around feature instead of only at only a location of feature. In general, the final extracted bit in this case has been decided as below:

$$b' = \begin{cases} 0, & NUM_0 \geq NUM_1 \\ 1, & NUM_0 < NUM_1 \end{cases} \quad (8)$$

where NUM_0 and NUM_1 is the total number of bits 0s and 1s in the extracted area from (8).

C. Scale-Invariant Feature Transform

The idea of solving the robustness problem of embedded information is to look for features in the image that are invariant to attacks. The information is then embedded based on these features. The local invariants must be highly distinguishable from others and suitable for their resistance to attacks. In the embedded information synchronization based on the image content, the robustness of feature extraction is related to the robustness of the watermarking system, and examining the local features is helpful in extracting the features. By combining the embedded information with image content-based features, the information extraction process can be performed flawlessly. Recently, the SIFT (Scale-Invariant Feature Transform) is one of the most efficient methods of extracting robust features [20]-[22]. It was invented by David Lowe since 2004 and up to now, there have been many improvements in the algorithm as well as the application in images. SIFT features are localized in scale-space according to pyramid filtering, separated from each other by four parameters including coordinates (*p, q*), coefficients of scaling (σ) and orientation (θ), as well as a description (size of 1×128) as shown in Fig. 1. It has proven to be invariant with rotation, scaling, and translation. It is also partially constant for changes in brightness and noise.

The main idea of the SIFT based watermarking is to extract features in a scale space. Information is then embedded in the circles centered at the feature point's location and the radius is proportional to the scale coefficient. Based on SIFT, Nikolaidis [23] uses all the features to embed the watermark so that the synchronization problem is preserved. However, the large number of embedded regions required by the algorithm degrade the quality of the embedded image. Also, not all features are useful for embedding and extracting information. Therefore, Guo, Li and Pan [24] selected only a few robust features to embed information using the quantization algorithm and have shown efficacy compared to previous methods. However, the original information is required from the extraction process by this method. In addition, by using the same algorithm to select a robust embedded area during the embedding and extraction process, it may lead to loss of synchronization during extraction. On the other hand, some authors improve synchronization by adding orientation characteristics. However, they also need to know in advance the original descriptions of the embedded features in the extraction. Moreover, most existing medical image watermarking methods focus on one-bit information embedding or do not consider fully attacks including both types of synchronization and non-synchronization. Furthermore, they lack a security mechanism to prevent illegal detection or extraction of information as well as the reliability evaluation of the extracted information. Therefore, in this

paper, we propose a new solution to overcome these disadvantages.

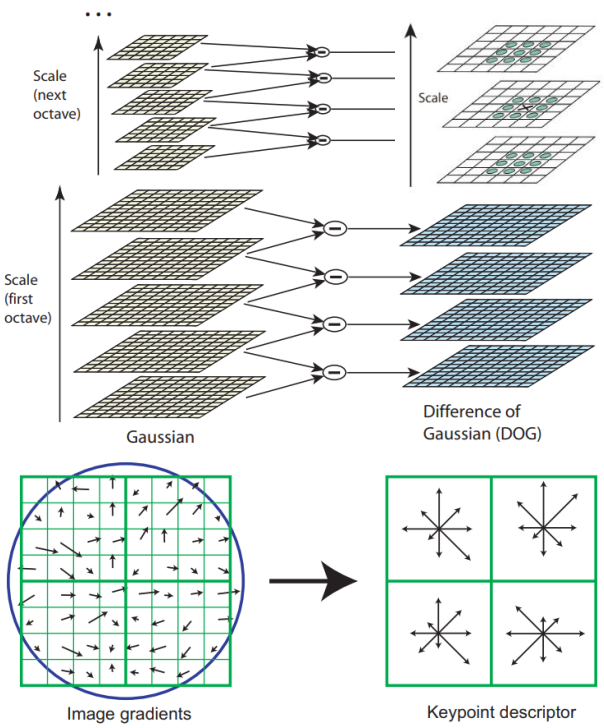

Figure 1. SIFT keypoints.

The rest of this paper is organized as follows. In Section III, our solution for robust blind image watermarking by combination of quantization technique and SIFT keypoints is proposed. First, process of embedding and extracting information is introduced and analyzed. Second, the expansion for multi-bit watermarking with two suggestions of fan-shaped and half-ring-shaped regions is mentioned. Next, the solution to enhance the security of extracting information is discussed. Experimental results with medical images are provided in Section IV to evaluate the quality, reliability, and robustness. Section V summarizes and concludes the paper.

III. Proposed Solution

A. The Process of Embedding Information

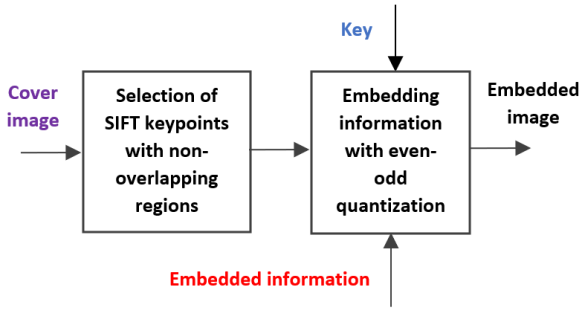

Figure 2. The process of embedding information.

The embedding algorithm is proposed in Fig. 2. First, SIFT is applied to the cover image to extract features. However, these features are not directly used to embed information, because they may cause overlapping regions. Instead, we need to determine the suitable features for efficient embedding by selection of non-overlapping regions and removal of features near borders. Information is then embedded into circular regions according to the features' coordinates and scale coefficients

$$(x-p)^2 + (y-q)^2 = (k\sigma)^2 \tag{9}$$

where, k is the amplification factor to control the radius of the circles. This factor is inversely proportional to scale coefficient so that the embedded areas are the same.

As we can see, for attacks such as rotation, scaling or translation, the closer the center of the image the position of the feature is, the more robust it is. Therefore, after removing the features that cause the embedding area to overflow out of the boundary, we will prioritize the feature with the closest coordinate to the center. The next step is to remove all features whose embedding area overlaps the embedding area of the selected feature. Repeat the same for the remaining features until none of the features overlap. Embedding process is effective when we select just enough robust features to embed. If there are too few embedding features, it will be difficult to correctly extract the embedded information. If there are too many embedding features, then the number of pixels of each embed area is too small, reducing the ability to extract the correct information when an attack significantly changes the pixel value of the embedded area.

B. The Process of Extracting Information

As (8), the reliability is the smallest (equal to 0.5) when the total number of bits 0s and 1s in the extracted area are equal and it is the largest (equal to 1) if all bits are only 0s or 1s. Correspondingly, the parameter for evaluating the reliability with the quantization method in this paper is then defined as below:

$$R_Q = \frac{\max\{NUM_0, NUM_1\}}{NUM_0 + NUM_1} \tag{10}$$

Furthermore, it is also clear that when extracting information corresponding to the actual embedding area, it will give the correct result with high bit rate (0 or 1). For the non-embedding region, when extracting information will give a random result with approximately the same bit rate 0 and 1. Therefore, based on a given threshold we can estimate the regions are more likely to be the initial embedding area. This is exploited in our paper to propose the extraction algorithm in Fig. 3.

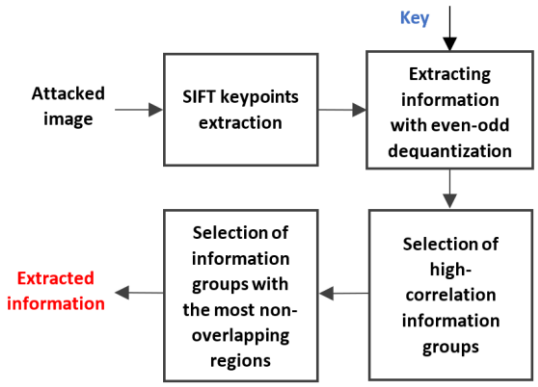

Figure 3. The process of extracting information.

Since there is no original image, selecting the embedded SIFT features from the attacked image is more challenging. Some embedded features may disappear as well as additional non-embedding features appear, making it difficult to correctly determine embedded areas. Therefore, the solution offers an algorithm to accurately select the original non-overlapping embedding regions based on the correlation comparison between the extracted information in all extraction regions before deciding the final extracted information. This algorithm begins by finding two extraction regions with the lowest correlation of extracted information, and then finding extraction regions with the high correlation of extracted information corresponding to these two extraction regions. In the case that there exist two groups of extracted regions with the corresponding information, the group with less features will be removed. If the number of features of the two groups is equal, discard the group with the smaller total area. In case no matching information is found, remove both extraction regions. This process is repeated until the last group of extraction regions used to extract information has been determined.

C. Expansion to Multi-bit Watermarking

The paper also suggests two embedded methods for multi-bit watermarking: (1) Each circular region will be divided into several small fan-shaped patches according to the length of information bit sequence. These patches are the same area as shown in Fig. 4. (2) Each circular region will be divided into several half-ring-shaped patches as shown in Fig. 5. Each half of patch is the same radius and corresponds to one information bit so that the number of ring-shaped patches is half of the length of information bit sequence.

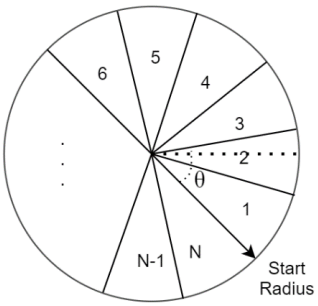

Figure 4. Fan-shaped patches.

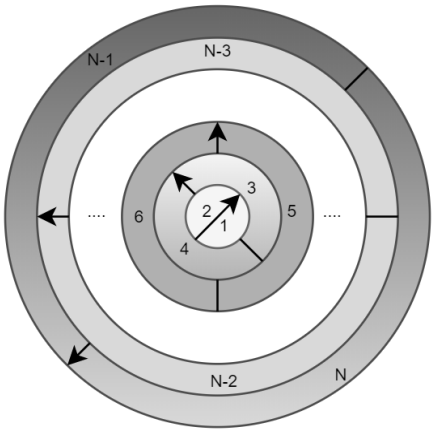

Figure 5. Half-ring-shaped patches.

For the method of embedding information in N fan-shaped patches, the embedding regions are defined as follows:

$$FS_i = \left\{(x,y) | -\theta + (i_1 - 1)\frac{2\pi}{N} \le \theta_{x,y} \le -\theta + i_1\frac{2\pi}{N}\right\} \quad (11)$$

where

$$\theta_{x,y} = arctan\left(\frac{y}{x}\right) \quad (12)$$

For the method of embedding information in N half-ring-shaped patches, the embedding regions (for each pair of bits) are defined as follows:

$$HRS_i = \left\{(x,y) \mid (i_2 - 1)\frac{2R_0}{N} \le p_{x,y} \le i_2\frac{2R_0}{N}\right\} \quad (13)$$

where

$$p_{x,y} = \sqrt{x^2 + y^2} \quad (14)$$

D. Solution for Enhanced Security

However, until now, there is the lack of a security mechanism because the embedded images are easily detected or extracted information by simple image analysis such as using histograms or de-quantization. Moreover, the embedded regions are located exactly around the features and location of the watermark would then be known to an attacker. Therefore, in our proposed method, we use a secret key to derive the embedded regions which cannot be determined in detection process without the same key. By using this secret key, both random angle α and random length γ are generated. Together, these yield the new location of the center of the embedded region by adding random angle α to the orientation factor θ of the feature and multiplying random length γ to the scale factor σ belonging to the feature as shown in Fig. 6.

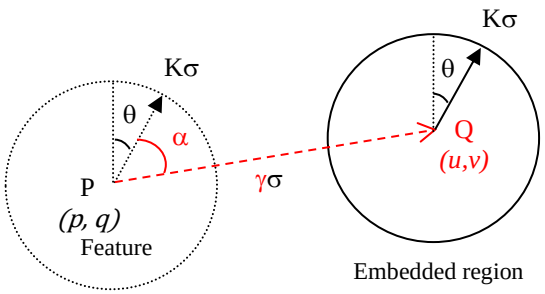

Figure 6. The embedded region derived from feature with a secret key.

To enhance the security for multi-bit watermarking, each patch is shifted by a random offset angle from a secret key with the initial point based on the orientation of feature. In the fan-shaped method, the shifting is the same for all patches while it can be different in the half-ring-shaped method. This helps to enhance the security of extracting information, which is one of requirements in medical field.

IV. Experimental Results

First, the paper investigates the watermarking properties of different medical images as shown in Table I. Correspondingly, the amplification factor is selected

properly to achieve the highest efficiency for extracting process.

TABLE I. WATERMARKING PROPERTIES OF DIFFERENT MEDICAL IMAGES

Image	XR	MRI	CT	US
Size	1024x1024	591x463	220x340	700x1024
Maximum scale	92.31	38.95	30.35	82.99
Number of embedded keypoints	14	21	10	13

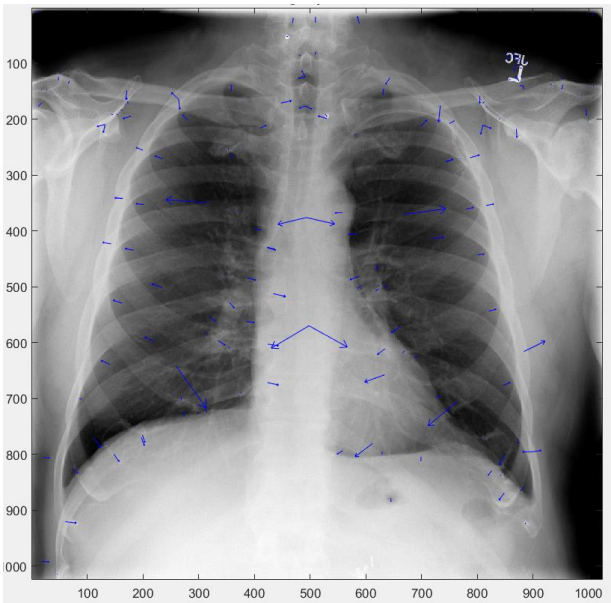

Figure 7. Original image with entire features.

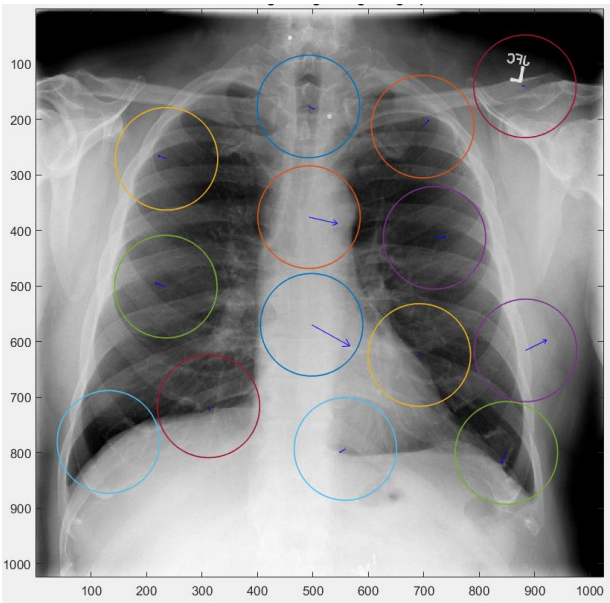

Figure 8. Embedded image with embedded regions correspondingly.

In order to achieve distinct threshold of perception by the human eye (more than 38dB), the embedding strength coefficient is chosen by α=3 in the spread spectrum-based method while the quantum interval Δ=5 with the quantization-based method. Fig. 7. shows the original image with entire features and Fig. 8. shows the embedded image with embedded regions correspondingly. The distortion between the embedded image and the original image is assessed by the quantities PSNR and SSIM as given in (6) and (7) with different watermarking solutions including SS and LSB, and shown in Table II. Obviously, the LSB method will give the highest quality of embedded image when evaluated by PSNR or SSIM, but is very sensitive with attacks, so it is only suitable for noiseless channel. Proposed method yields better embedded image quality than SS by embedding information only in regions corresponding to the selective robust features. On the other hand, when evaluated by SSIM, the embedded image quality of this method is approximated to LSB, which means imperceptibility.

TABLE II. COMPARISON OF THE QUALITY AND RELIABILITY OF DIFFERENT METHODS

Method	SS	LSB	Quantization (proposal)
PSNR (dB)	38.67	51.01	43.24
SSIM	0.8961	0.9928	0.9695

Table III shows the reliability of proposed quantization-based method for one-bit watermarking without attack and against various attacks. The detection or extraction process is successful if there is at least one region whose reliability is greater than a given threshold. For example, with the threshold greater than 0.6512, our solution can detect if this image is embedded while it obtains the robustness against most attacks in Table III except for the Gaussian noise.

TABLE III. COMPARISON OF RELIABILITY OF PROPOSED METHOD

Attack	Reliability (max)
None (embedded image)	1
None (original image)	0.6512
Average filtering	0.7814
Gaussian lowpass filtering	0.9493
Laplacian of Gaussian filtering	0.8824
Gaussian noise (0, 0.01)	0.6119
Salt & pepper noise (0.02)	0.9891
JPEG (quality of 100)	1
JPEG (quality of 75)	0.7468
JPEG2000	1
Rotation 90°	1
Rotation 1°	1
Rotation of 45°	1
Cropping 10%	1
Cropping 20%	1
Scaling of 0.2	0.7048
Scaling of 0.4	0.7465
Scaling of 0.6	0.7883
Scaling of 0.8	0.8373
Scaling of 1.2	0.8941
Scaling of 1.4	0.8928
Scaling of 1.5	0.8905
Scaling of 1.6	0.8726
Scaling of 1.8	0.8725
Scaling of 2	0.9480

V. CONCLUSION

In summary, the paper offers an effective solution for watermarking with common medical images by combining the quantization technique with the selection of proper non-overlapping SIFT features. In addition to fully

investigating two types of synchronization and non-synchronization attacks as well as evaluating the embedded image quality with different parameters including MSE, PSNR, SSIM, the article also examines the specific requirements in the medical field such as the reliability and the security. Moreover, proposed solution can embed not only one information bit but also multiple bits of information into the fan-shaped and half-ring-shaped patches. With the usage of a secret key in the division of the embedded region corresponding to the bits of information, the extraction process is enhanced for security. Especially, with the algorithm to determine the embedded regions based on the correlation of the received bit sequences, our proposed solution does not need to use the original image but still achieve high robustness. The simulation results show that the proposed solution achieve high resilience to various types of synchronization attacks as well as image filtering and compressions.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Tuan Nguyen-Thanh conducted the research, analyzed the solutions, and wrote the paper; Thuong Le-Tien supervised, conducted the research, and discussed the results; all authors had approved the final version.

ACKNOWLEDGMENT

This research is funded by Ho Chi Minh City Department of Science and Technology (DOSTHCM) under grant number 98/2019/HD-QPTKHCN. We would like to thank Ho Chi Minh City University of Technology (HCMUT), Vietnam National University Ho Chi Minh City (VNU-HCM) for the support of time and facilities for this study.

REFERENCES

[1] U. H. Panchal and R. Srivastava, "A comprehensive survey on digital image watermarking techniques," in *Proc. Fifth IEEE Int. Conf. Communication Systems and Network Technologies*, 2015, pp. 591-595.

[2] A. Ray and S. Roy, "Recent trends in image watermarking techniques for copyright protection: a survey," *Int. J. Multimed. Info. Retr.*, vol. 9, pp. 249-270, 2020.

[3] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: A survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714-729, 2014.

[4] X. Guo and T. Zhuang, "A lossless watermarking scheme for enhancing security of medical data in PACS," *Medical Imaging: PACS and Integrated Medical Information Systems*, pp. 350-359, 2003.

[5] H. M. Chao, C. M. Hsu, and S. G. Miaou, "Data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Information Technology in Biomedicine*, vol. 6, no. 1, pp. 46-53, 2002.

[6] A. Nikolaidis, S. Tsekeridou, A. Tefas, and V. Solachidis, "A survey on watermarking application scenarios and related attacks," in *Proc. Int. Conf. Image Processing*, 2001, vol. 3, pp. 991-994.

[7] B. Kumar, S. B. Kumar, and D. S. Chauhan, "Wavelet based imperceptible medical image watermarking using spread-spectrum," in *Proc. 38th IEEE Int. Conf. Telecommunications and Signal Processing*, 2015, pp. 1-5.

[8] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72-80, 2020.

[9] S. Kushlev and R. P. Mironov, "Analysis for watermark in medical image using watermarking with wavelet transform and DCT," in *Proc. 55th International Scientific Conference on Information, Communication and Energy Systems and Technologies*, 2020, pp. 185-188.

[10] K. Singh, B. Kumar, M. Dave, and A. Mohan, "Multiple watermarking on medical images using selective DWT coefficients," *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, pp. 607-614, 2015.

[11] R. Nilesh and H. Ganga. "Securing medical images by watermarking using DWT-DCT-SVD," *International Journal of Computer Trends and Technology*, vol. 10, pp. 1-9, 2014.

[12] X. Q. Zhou, H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Trans. Medical Imaging*, vol. 20, no. 8, pp. 784-791, 2001.

[13] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimed. Tools Appl.*, vol. 76, pp. 3669-3697 2017.

[14] J. Cox, J. Kilian, F. T. Leighton, and G. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[15] H. S. Malvar and D. A. F. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Processing*, vol. 52, no. 4, pp. 898-905, 2003.

[16] Y. Erfani and S. Ghaemmaghami, "Improving robustness of iss watermarking against malicious attack," in *Proc. IEEE Int. Conf. Computational Intelligence*, vol. 1, pp. 497-501, 2004.

[17] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423-1443, 2001.

[18] A. Z. Tirkel, G. A. Rankin, R. V. Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne, "Electronic water mark," in *Proc. Digital Image Computing, Technology and Applications*, 1993, pp. 666-672.

[19] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. on Image Processing*, 1994, pp. 86-90.

[20] P. Bollimpalli, N. Sahu, and A. Sur, "SIFT based robust image watermarking resistant to resolution scaling," in *Proc. IEEE Int. Conf. Image Processing*, 2014, pp. 5507-5511.

[21] X. Wang and W. Tan, "An improved geometrical attack robust digital watermarking algorithm based on SIFT," in *Proc. the 6th International Asia Conference on Industrial Engineering and Management Innovation*, 2016, pp. 209-217.

[22] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004.

[23] A. Nikolaidis, "Local distortion resistant image watermarking relying on salient feature extraction," *Journal on Advances in Signal Processing*, pp. 1-17, 2012.

[24] B. L. Guo, L. D. Li, and J. S. Pan, "Robust image watermarking based on scale-space feature points," *Information Hiding and Applications*, pp. 75-114, 2009.

Tuan Nguyen-Thanh was born in Ho Chi Minh City, Vietnam. He received B.Eng. and M.Eng. degrees from Ho Chi Minh City University of Technology (HCMUT), Vietnam, in 2002 and 2004, respectively, both in electrical engineering and telecommunications. He has been at the HCMUT since 2002. Currently, he is pursuing the Ph.D. degree at the HCMUT, under the supervision of Prof. Thuong T. Le. His main research interests include watermarking, digital signal processing and communication systems.

Thuong Le-Tien (MIEEE-96) was born in Saigon, Ho Chi Minh City, Vietnam. He received the Bachelor and Master Degrees in Electronics-Engineering from Ho Chi Minh City Uni. of Technology (HCMUT), Vietnam, then the Ph.D. in Telecommunications from the Uni. of Tasmania, Australia. Since May 1981 he has been with the EEE Department at the HCMUT. He spent 3 years in the Federal Republic of Germany as a visiting scholar at the Ruhr Uni. from 1989-1992. He served as Deputy Department Head for many years and had been the Telecommunications Department Head from 1998 until 2002. He had also appointed for the second position as the Director of Center for Overseas Studies since 1998 up to May 2010. His areas of specialization include: Communication Systems, Signal Processing and Electronic Circuits. He has published more than 190 scientific articles and the teaching materials for university students related to Electronic Circuits 1 and 2, Digital Signal Processing and Wavelets, Antenna and Wave Propagation, Communication Systems. Currently he is a full professor at the HCMUT.