Journal of Advances in Information Technology Vol. 11, No. 3, August 2020

Study on Improved Cooperative Spread Spectrum Based Robust Blind Image Watermarking

Tuan Nguyen-Thanh and Thuong Le-Tien
Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam
Vietnam National University Ho Chi Minh City (VNU-HCM), Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Vietnam
Email: {nttuan, thuongle}@hcmut.edu.vn

Abstract—**Spread Spectrum (SS) is one of the most common techniques used in watermarking systems due to its security, robustness, imperceptibility and information extracting without the host data. However, this technique suffers the interference between the host data and the watermark, which degrades significantly the performance of watermarking system. In the other hand, most existing spread spectrum-based image watermarking methods are non-blind and implemented for single channel images with one information bit. Therefore, this paper presents a new cooperative spread spectrum based blind watermarking technique, which can apply to not only single channel images but also multi-channel images or set of images. In this technique, the same information is embedded into multiple channels and a global linear cooperative decision is used to exploit the collaboration among the local correlation detectors. Moreover, improved method is also mentioned to eliminate the interference between the host images and the watermarks. Especially, the Karhunen Loeve Transform (KLT) is exploited to enhance the performance of the proposed cooperative watermarking system. Furthermore, extensive methods for multi-bit watermarking are also discussed. Based on theoretical analysis, the optimal solutions of the watermark, watermark strength coefficients, weighting coefficients, threshold, and probability error are established. Experimental results are simulated with ideal channel (without attack) as well as additive Gaussian channel to verify theoretical analysis.**

Index Terms—**robust blind image watermarking, spread spectrum, correlation, Karhunen Loeve Transform**

I. INTRODUCTION

Watermarking technology has been developed rapidly in recent years and is constantly expanding its applications such as copyright protection, copy control, data authentication, fingerprinting, indexing, broadcast monitoring, secure communication, etc., to become one of the advanced information hiding techniques. In general, the basic idea of watermarking is to embed and extract information (or watermark) in multimedia data (also called original data or cover data or host data). Based on communication theory, a typical watermarking system consists of three main parts: transmitter (or embedder) for embedding information, channel for attacks and receiver (or detector) for extracting information. The data after embedding is called the embedded data (or watermarked data). This data can be attacked through channel, which are then called attacked data (or received data).

There are many different criteria for classifying watermarking techniques [1]. In general, a watermarking system usually includes the following basic characteristics:

- Quality (imperceptibility): only small changes to the original data to ensure that the embedded data cannot be perceived by the human eye or ear.
- Robustness: ability to extract information successfully against attacks.
- Capacity: the amount of embedded information.
- Security: extracting information only with valid users.
- Blind: extracting information without host data.
- Complexity: difficult level for implementation of embedding and extracting processes.

Therefore, for accurate results, it is necessary to ensure that the methods used for the survey are evaluated under the same criteria. In addition, depending on the requirements of each application, the goals of the watermarking system design will vary. In general, the watermarking system design problem is a challenging task. Therefore, although there are many watermarking methods with different advantages, each method still has certain limitations.

Although watermarking can be applied to multimedia data such as images, audio, video sequences, etc., this paper only focuses on image watermarking. The first studies of image watermarking were carried out directly in the spatial domain based on the gray scale value adjustment methods, where the Least Significant Bit (LSB) method is the most simple and common [2]. Because the information is embedded in the low-weight bits of pixels of the cover data, this method obtains the high capacity of the embedded information and the good imperceptibility of the embedded data. The process of embedding and extracting information of the LSB method is implemented very simple. However, the security and robustness of this method is very low. It is only suitable to applications with reliable channel (without attack).

Manuscript received February 15, 2020; revised July 3, 2020.

doi: 10.12720/jait.11.3.119-127

Before the attacks appear more and more in the channel, especially the usage of the lossy image compression algorithms such as JPEG and JPEG2000, the introduction of new watermark techniques applied in the transform domain in order to solve the above problem [3]-[5]. The main purpose of these techniques is to transfer image data from the spatial domain to other domains such as DCT and DWT for embedding and extracting the information, where the embedded information will be more robust against attacks, e.g., JPEG and JPEG2000 compression techniques. Moreover, due to the human visual system, the imperceptibility can be improved significantly in transform domains. Therefore, most methods for image watermarking are exploited in transform domains.

By analyzing the watermarking system according to the communication model, it has opened up many opportunities for applying communication techniques to enhance the watermarking process. In the field of radio communication, the spread spectrum technique is heavily applied by its security. The idea of the spread spectrum based watermarking algorithm is to use a Pseudo-Random Noise (PRN) generator for embedding and extracting the information. Based on multiple access capability, this technique allows each person to perform the embedding process to have their own key. The information will then be extracted from the embedded data or attacked data with the same key. That means only user having the key used in the embedding process can extract accurately the embedded information in the cover data. Besides, because the embedded information will be spread over the entire cover data, the transparency of the embedded information will be completely guaranteed [6]. Moreover, because this technique can be applied in transform domains of image data, the invisibility in the embedded images and robustness of the embedded information against attacks will be greatly increased. Because of these characteristics, the spread spectrum based watermarking is still being researched and developed in many applications [7]-[14].

Although there are different methods in spread spectrum-based watermarking, in general, it can be classified into blind and non-blind (or obvious) approaches. Most improved solutions to obtain good results were applied for non-blind approach, which requires host data to extract the embedded information. Meanwhile, the blind spread spectrum-based watermarking suffers interference between the host data and the watermark, which reduces the reliability and robustness of watermarking system. Another issue is the lack of theoretical analysis for image watermarking, where many authors focused on different algorithms for certain image data and selected the parameters mainly through experiments. In addition, most watermarking techniques applied to single channel images, particularly common grayscale images. The number of watermarking studies for multiple channel images such as color images, medical images or set of images was limited. Furthermore, with image watermarking system, especially in transform domains, rounding errors and practical limitation of PRN generator are also factors that affect the accuracy.

II. RELATED WORKS

In the early 1990s, watermarking technology began to receive attention and developed rapidly in many areas such as copyright protection, copy control, data authentication, fingerprinting, indexing, broadcast monitoring and data hiding. The first studies of image watermarking were carried out directly in the spatial domain based on the gray scale value adjustment methods. The LSB replacement technique was proposed by Schyndel *et al.* [15] by embedding watermark as binary random string into the remaining LSB of the image after 7-bit gray level histogram compression and using bit sequence comparators to detect watermark. Other authors embed binary information directly in LSB planes of images. Because LSBs carry little information and negligible impact on image quality, this technique achieves high embedded information capacity and good imperceptible embedded image.

Cox *et al.* [16] were the first authors to exploit the spread media theory to build a watermarking algorithm. They embedded a watermark with a Gaussian distribution in the lowest DCT coefficients of the image. Watermark is restored by subtracting the original image from the embedded image and calculating the similarity between the restored watermark and the original one. This technique is quite robust but not suitable for many applications in practice because it requires original host images in extracting process. Instead, other authors used the blind spread spectrum based watermarking technique [7], [9], [12]. The basic idea of this approach is using bipolar random sequence as watermark. This sequence is generated from a pseudo-random noise generator through a key. The embedded information is extracted using the correlation detector with the same embedded key. As such, the security of watermarking system greatly increases compared to other techniques. By spreading the watermark into whole the host data, this method also achieves transparency and imperceptibility. In addition, spread spectrum based watermarking techniques can be implemented directly in the spatial domain or other transform domains such as DFT, DCT or DWT in order to improve the robustness against attacks [3], [14].

However, in spread spectrum based watermarking techniques, the host data itself is considered as a source of interference, which can cause significant errors in the extracting process. Therefore, Malvar and Florencio [17] proposed an improved spread spectrum technique to overcome the limitation in traditional spread spectrum based watermarking system. However, the distortion in the embedded image increases correspondingly. Moreover, only a bit of information is embedded in this technique.

In addition, although many watermarking techniques have been widely studied, the expansion of watermarking for multi-channel data such as color images, medical images or set of images still presents many opportunities and challenges. In most cases, this expansion is implemented by embedding the watermark directly into a specific image channel, such as the blue channel in the

RGB color space, or the brightness channel in YUV color space [2]. In contrast, Barni *et al.* [18] exploited the cross correlation of RGB color channels by designing a global correlation-based detector to synthesize information obtained from all three color-channels to improve the performance of the watermarking system. However, this technique only considers the average combination in the global detector and requires host data in extracting process. Currently, Hajjaji *et al.* [19] exploited the completely decorrelation property of the KLT to embed watermark for medical images. Unfortunately, a limitation of the KLT is that it depends on the statistical properties of the original data. As a result, the extracting process needs the host data, so the watermarking system is non-blind.

Therefore, in this paper, a new blind cooperative spread spectrum-based watermarking using the KLT is proposed to reduce or eliminate the interference between the host images and the watermark. In our technique, the same information is embedded into multiple channels and a global linear cooperative decision is used to exploit the collaboration among the local correlation detectors. Unlike existing methods, by using orthogonal watermarks, the embedded information can be extracted successfully without the host data.

The rest of this paper is organized as follows. In Section III, the results based theoretical analysis are derived to helps us understand in detail the performance of the proposed watermarking methods, including the optimal solutions, practical limitations of blind image watermarking and different applications. First, the traditional spread spectrum based blind watermarking is reviewed. Second, the proposed cooperative spread spectrum based blind watermarking technique is introduced and analyzed. Next, the improved method is mentioned to eliminate the interference between the host images and the watermark. After that, the proposal of the KLT in the embedding and extracting processes is presented, especially the condition for perfect reconstruction of the KLT without the host signal is established. The last part of this section is the expansion of the proposed methods to the multi-bit watermarking. Experimental results are provided in Section IV to verify theoretical analysis. Section V summarizes and concludes the paper.

III. THEORETICAL ANALYSIS

A. *Analysis of Embedding and Extracting Process of Traditional SS-based Blind Watermarking*

In this paper, the model of traditional additive direct sequence SS-based blind watermarking is considered as shown in Fig. 1. A secret key *K* is used by a PRN generator to produce a sequence *U*. This sequence, also called as the watermark, is used in both embedding and extracting processes to embed and extract the information bit *b*. The system is blind so there is not host signal in the receiver.

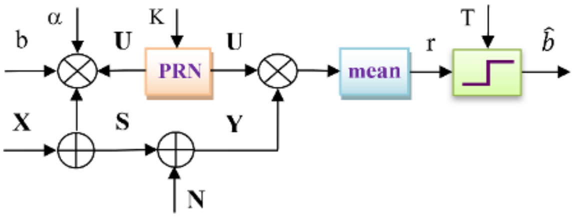

Figure 1. Traditional SS-based blind watermarking scheme.

To be able to analyze the watermarking process more easily, let us use the notation E[*A*] (or $\bar{A}$) for the mean (average) value of signal *A*.

Without loss of generality, assume that the random watermark *U* is zero-mean and normalized in whole this paper, i.e.,

$$E[U]=0 \tag{1a}$$

$$E[U.U]=1 \tag{1b}$$

In the embedding process, the watermark *U* is added to the host signal *X* according to the information bit transmitted *b* and the watermark strength α to obtain the embedded signal *S* as shown in (2).

$$S = X + b.\alpha.U \tag{2}$$

The mean square error (MSE) metric is used to evaluate the distortion *D* between the embedded signal and the host signal.

$$D = E[(X-S)^2] \tag{3}$$

Consider the attack in channel is additive Gaussian noise, i.e., $N \sim N(0, \sigma_n^2)$, then the attacked image *Y* at input of the receiver is

$$Y = S + N \tag{4}$$

In the extracting process, the mean (average) value *r* of a multiplication between the received signal and the watermark is calculated to decide the information bit $\hat{b}$ based on a given threshold *T*. This calculation is similar to the correlation in signal processing or inner product in linear algebra as shown in (5a).

$$r = E[(Y-\bar{Y}).(U-\bar{U})] \tag{5a}$$

If the condition in (1a) is satisfied, (5a) can be reduced to

$$r = E[Y.U] \tag{5b}$$

If the condition in (1b) is satisfied, (5b) becomes

$$r = E[X.U] + b.\alpha + E[N.U] \tag{5c}$$

By using only a simple correlation detector without host signal (thus called the blind watermarking), the SS-based watermarking is easily implemented in hardware and suitable to many practical applications. However, the correlation between the host signal and the watermark in (5c) now becomes a source of interference. This degrades the performance of the watermarking system. Even in the absence of an attack, the error still exists in traditional SS-based blind watermarking. To evaluate the probability of error, we need to estimate the distribution of the correlation coefficient r in (5c).

For theoretical analysis, assume the host signal also has Gaussian distribution, i.e., $X \sim \mathrm{N}(m_x, \sigma_x^2)$. Then, the correlation coefficient is also a Gaussian distribution, i.e., $r \sim \mathrm{N}(m_r, \sigma_r^2)$ with the mean and variance given by following equations.

$$m_r = b.\alpha \tag{6}$$

$$\sigma_r^2 = \sigma_x^2 + \sigma_n^2 \tag{7}$$

From (6) and (7), we have the optimal threshold T for decision when embedding the information bit $b = \{b_1, b_2\}$ and the error probability p correspondingly as below.

$$T = \frac{b_1 + b_2}{2}.\alpha \tag{8}$$

$$p = \frac{1}{2} erfc\left(\frac{|b_1 - b_2|.\alpha}{2\sqrt{2}.\sigma_r}\right) \tag{9}$$

where *erfc(.)* is the complementary error function.

In the case of the information bit $b=\{0/1\}$ then the threshold becomes α/2, depending on the watermark strength. Actually, in this case, the watermark is embedded to host signal or not corresponding to the state of the information bit. It is commonly used to decide whether a given watermark is existed in a received signal or not. The main applications for this case are copyright protection, copy control.

In the case of the information bit $b=\{\pm 1\}$, i.e., a given watermark is always embedded into a host signal but in two different forms, depending on the state of the information bit. The advantage of this case is that the threshold is fixed to zero, independent to the watermark strength. It means the extracted bit is the sign of the correlation value of the detector. However, this case is only used to extract the information from given embedded signals. It means the receiver cannot work properly with any input signal is not watermarked. The following results in this paper are derived for this case.

It is also noted that, in fact, the host images are always not zero-mean. However, only with the requirement of the zero-mean watermark, (5c) is always obtained with image data. This requirement is necessary in order to derive the optimal threshold in (8). If not, the optimal threshold will depend on the host image. Consequently, it is not efficient with the blind image watermarking.

Finally, we consider the security of this watermarking system. If the invalid users try to extract the embedded information with a different watermark U' corresponding to a different key, the correlation value for decision is now determined by

$$r' = E[X.U'] + b.\alpha.E[U.U'] + E[N.U'] \tag{10}$$

From (10), it is clear that in order to prevent to extract the embedded information in this case, the correlation between two different watermark needs to be zero, i.e.,

$$E[U.U'] = 0 \tag{11}$$

The condition in (11) is also called orthogonal.

B. Analysis of Embedding and Extracting Process of Cooperative SS-based Blind Watermarking

We consider the embedding and extracting process of the general cooperative spread spectrum based blind watermarking system for m image channels as shown in Fig. 2.

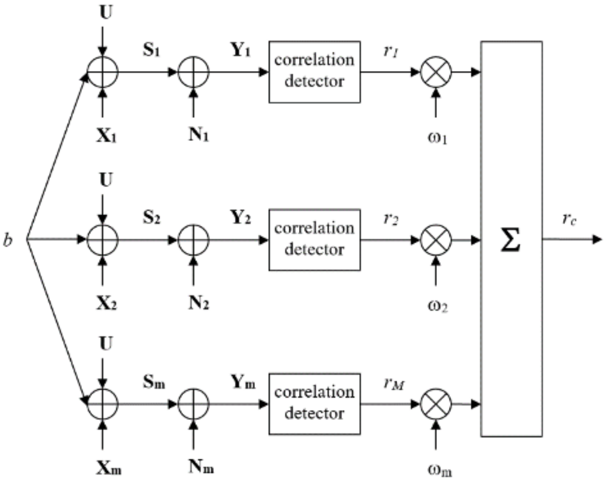

Figure 2. Cooperative SS-based blind watermarking scheme.

In the embedding process, the normalized random watermark U is added to each host image channel X_i according to the information bit $b=\{\pm 1\}$ and the strength factor α_i to obtain each embedded image channel S_i as below.

$$S_i = X_i + b.\alpha_i.U \tag{12}$$

In the extracting process, like the traditional spread spectrum base watermarking, the local correlation r_i from each channel is also determined by

$$r_i = E[Y_i.U] = E[X_i.U] + b.\alpha_i + E[N_i.U] \tag{13}$$

Unlike the traditional spread spectrum-based watermarking, a linear combination is exploited in the global detector of the cooperative watermarking system as shown in (14).

$$r_c = \sum_{i=1}^{m} w_i.r_i \tag{14}$$

where $\{w_i \geq 0\}$ are the weighting coefficients used to control the global detector from the local correlation detectors.

The extracted bit is then decided by comparing the global cooperative correlation with a given threshold.

It is clear that the correlation value in each local detector is also Gaussian process, i.e., $r_i \sim \mathrm{N}(m_{ri}, \sigma_{ri}^2)$ with the mean and variance given by following equations.

$$m_{ri} = b.\alpha_i \tag{15a}$$

$$\sigma_{ri}^2 = \sigma_{xi}^2 + \sigma_{ni}^2 \tag{15b}$$

Consequently, their linear combination is also Gaussian with the mean and variance given by following equations.

$$m_{rc} = \sum_{i=1}^{m} w_i.m_{ri} = b\sum_{i=1}^{m} w_i.\alpha_i \tag{16a}$$

$$\sigma_{rc}^2 = \sum_{i=1}^{m} w_i^2.\sigma_{ri}^2 \tag{16b}$$

Then, the error probability of the proposed watermarking system can be evaluated as

$$p_c = \frac{1}{2} erfc\left(\frac{\sum_{i=1}^{m} w_i.\alpha_i}{\sqrt{2}\sqrt{\sum_{i=1}^{m} w_i^2.\sigma_{ri}^2}} \right) \tag{17}$$

From (17), the close-form expressions for minimum error probability and optimal weighting coefficients correspondingly are derived as the following equations.

$$p_{opt} = \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \sqrt{\sum_{i=1}^{m} \frac{\alpha_i^2}{\sigma_{ri}^2}} \right) \tag{18}$$

$$\frac{w_i^{opt}}{w_j^{opt}} = \frac{\alpha_i}{\alpha_j}\frac{\sigma_{rj}^2}{\sigma_{ri}^2} \tag{19}$$

Next, we consider the performance of the optimal cooperative detector in some special cases of the watermark strength. Table I shows the error probability for different selections of the watermark strength.

TABLE I. ERROR PROBABILITY OF THE OPTIMAL COOPERATIVE DETECTOR FOR DIFFERENT SELECTIONS OF THE WATERMARK STRENGTH

Watermark strength	**Error probability**
$\alpha_i = \alpha_j = \sqrt{D}$	$\frac{1}{2}\text{erfc}\left(\frac{\sqrt{D}}{\sqrt{2}}\sqrt{\sum_{i=1}^{m}\frac{1}{\sigma_{r_i}^2}}\right)$
$\frac{\alpha_i}{\alpha_j} = \frac{\sigma_{r_i}^2}{\sigma_{r_j}^2}$	$\frac{1}{2}\text{erfc}\left(\frac{\sqrt{D}\sqrt{\sum_{i=1}^{m}\sigma_{r_i}^2}}{\sqrt{2}\sqrt{\sum_{i=1}^{m}\sigma_{r_i}^4}}\right)$
$\frac{\alpha_i}{\alpha_j} = \frac{\sigma_{r_i}}{\sigma_{r_j}}$	$\frac{1}{2}\text{erfc}\left(\frac{\sqrt{D}\sqrt{m}}{\sqrt{2}\sqrt{\sum_{i=1}^{m}\sigma_{r_i}^2}}\right)$

Furthermore, we also evaluate the average cooperative detector in which weighting coefficients are the same. The error probability in this case is given by

$$p_{ave} = \frac{1}{2} erfc\left(\frac{\sum_{i=1}^{m} \alpha_i}{\sqrt{2}\sqrt{\sum_{i=1}^{m} \sigma_{ri}^2}} \right) \tag{20}$$

C. Elimination of the Interference between the Host Signal and the Watermark

In order to eliminate the interference from the host signal, based on Malvar's method, only the embedding process is improved as below.

$$S^{imp} = X_i + b.\alpha_i.U - E[X_i.U].U \tag{21}$$

In the extracting process, the local correlation from each channel is still determined by

$$r_i^{imp} = E[Y_i.U] = b.\alpha_i + E[N_i.U] \tag{22}$$

It can be seen that the interference is now removed completely in (22) compared to that in (13). However, the distortion between the embedded signal and the host signal also increases greatly with this solution. Moreover, it cannot be applied in spatial domain of the host image due to the significant effect of the rounding error. To overcome these disadvantages, the transform domains are considered and exploited.

D. Exploitation of the KLT

In order to improve the quality of the embedded images, transform domains such as DCT, DWT can be used to embed and extract the information bit. These transforms are commonly used directly with individual images; thus, it is easy to apply for the cooperative watermarking system. Unlike these transforms, the KLT is based on multiple images. Therefore, in this paper, we especially exploit the KLT to improve the performance of proposed cooperative watermarking system.

The embedding process of proposed spread spectrum based watermarking system using the KLT is shown in Fig. 3. Let X = $[X_1, X_2, ..., X_m]^T$ be the vector containing m components corresponding to the number of host image channels.

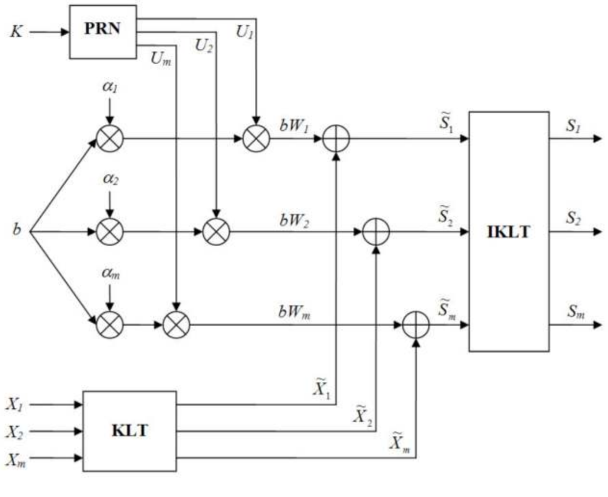

Figure 3. Improved cooperative SS-based embedding scheme using KLT.

Firstly, this host image set is completely decorrelated using KLT as

$$\tilde{X} = \begin{bmatrix} \tilde{X}_1 \\ \tilde{X}_2 \\ ... \\ \tilde{X}_m \end{bmatrix} = \Phi_X^T.X = \begin{bmatrix} \phi_{X_1}^T \\ \phi_{X_2}^T \\ ... \\ \phi_{X_m}^T \end{bmatrix}.X \tag{23}$$

where $\Phi_{X_i}^T$ is the eigenvector corresponding to the i-th eigenvalue λ_{X_i} of the covariance matrix $\sum_X$ of the vector X, i.e.,

$$\Sigma_X.\phi_{X_i} = \lambda_{X_i}.\phi_{X_i} \tag{24}$$

Next, a secret key K is used by a PRN generator to produce the orthogonal watermark sequences U = $[U_1, U_2, ..., U_m]^T$ for channels. This is the main difference in using the cooperative watermarking system with the KLT when compared to the spatial domain or any other transform domain. In those methods, we can use the same watermark for each channel. The condition of orthogonal watermarks in embedding process will prove to be the condition for the perfect reconstruction of the KLT in the blind extracting process.

Each sequence U_i is then added to each component $\tilde{X}_i$ of eigen-signal $\tilde{X}$ according to the information bit b and the strength factor α_i as shown in (25)

$$\tilde{S}_i = \tilde{X}_i + b.\alpha_i.U_i = \tilde{X}_i + b.W_i \tag{25}$$

Finally, the inverse KLT is used to obtain the watermarked data.

$$S = \Phi_X.\tilde{S} = \sum_{i=1}^{m} \tilde{S}_i.\phi_i \tag{26}$$

The extracting process of proposed spread spectrum based watermarking system using the KLT is shown in Fig. 4.

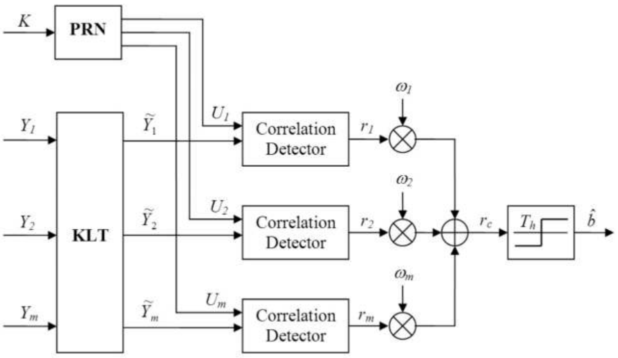

Figure 4. Improved cooperative SS-based extracting scheme using KLT.

On this side, the KLT is used again with the received signal Y to obtain the Eigen-signal $\tilde{Y}$ as the following expression.

$$\tilde{Y} = \Phi_Y^T.Y = \tilde{S} + \tilde{N} \tag{27}$$

Next, each component $\tilde{Y}_i$ of the Eigen-signal is brought to each local detector to determine the correlation from each channel as shown in (28).

$$r_i^{KLT} = E[\tilde{Y}_i.U_i] = E[\tilde{X}_i.U_i] + b.\alpha_i + E[\tilde{N}_i.U_i] \tag{28}$$

As we can see, when watermarking is implemented in transform domains, the calculations are not performed directly with the host images but their transformed coefficients. In particular, with the KLT, the interference comes from the correlation between the Eigen-images of the host images and the watermark. In addition, the effect of the Gaussian noise is converted to the effect of the Eigen-noise. Moreover, the distortion by the embedding process is determined with Eigen-images instead of host images. These characteristics can help to improve the robustness as well as the invisibility of the watermarking system.

It is noted that, for the embedding process, the KLT is based on the host data, whereas it is reconstructed from the watermarked data without the host data in the extracting process. Therefore, it is important to design the watermark so that it has no effect on the reconstruction of the KLT in the blind extracting process at least in the case of the absence of attack in order to ensure the reliability of the watermarking system. It is clear that the condition for the perfect reconstruction of the KLT is given by

$$\Phi_Y = \Phi_S = \Phi_X \tag{29}$$

Substitute this condition to the inverse KLT in (27) we have

$$Y = S + N = X + b.\Phi_X.W + N \tag{30}$$

Then the covariance matrix of the vector Y is calculated as

$$\Sigma_Y = \Sigma_S + \Sigma_N = \Sigma_X + \Phi_X.\Sigma_W.\Phi_X^T + \Sigma_N \tag{31}$$

Furthermore, since $\sum_X$ is symmetric matrix and Φ_X is orthogonal matrix, i.e., $\Phi_X^T = \Phi_X^{-1}$, so we have

$$\Phi_X^T.\Sigma_Y.\Phi_X = D_X + \Sigma_W + \Sigma_N \tag{32}$$

where D_X is the diagonal matrix corresponding to the eigenvalues $\{\lambda_{X_1}, \lambda_{X_2}, \lambda_{X_m}\}$.

Obviously, the condition in (29) is satisfied if and only if $\sum_W$ and $\sum_N$ in (32) are diagonal. These are equivalent to the orthogonal watermarks the additive Gaussian attacks. Thus, by designing the orthogonal watermarks, the perfect reconstruction for the KLT in the blind extracting process is satisfied in both cases, channel without attack and additive Gaussian channel. This can be implemented by utilizing Hadamard matrix [13].

E. Expansion to the Multi-bit Watermarking

The proposed methods above are only mentioned for single information bit. In order to embed multiple bits of information, we can segment images into smaller blocks and perform watermarking for each of these blocks. Although the proposed cooperative spread spectrum based watermarking systems are developed for multiple channel images, single channel images can be also applied by image block division solution. However, the capacity of the embedded information by this solution depends on the limitation of the host image size and the watermark length in practice. The relationship between the block size and the embedded information bit capacity as well as the watermark length is given in Table II in the case of 512×512 images.

TABLE II. WATERMARK LENGTH (IN THE CASE OF 512×512 IMAGES)

Block size	Capacity	Watermark length
8x8	4096	64
16x16	1024	256
32x32	256	1024
64x64	64	4096
128x128	16	16384

Another solution for multi-bit watermarking is embedding multiple bits $\{b_1, b_2, \ldots, b_B\}$ into the same host image channel with different watermark is given in (33). It is noted that, we can apply this solution for spatial domain or any transform domain, even with the KLT in this paper.

$$S_i = X_i + \sum_{k=1}^{B} b_k.\alpha_{ik}.U_{ik} \tag{33}$$

In this case, the local correlation for extracting each bit b_k from each channel is determined by

$$r_{ik} = \sum_{k=1}^{B} E[Y_i.U_{ik}] = \sum_{k=1}^{B} E[X_i.U_{ik}] + \sum_{k=1}^{B} b_k.\alpha_{ik} + \sum_{k=1,n=1,k\neq n}^{B} b_k.\alpha_{ik}.E[U_{ik}.U_{in}] + \sum_{k=1}^{B} E[N_i.U_{ik}] \tag{34}$$

From (34), to obtain the reliability as that of single bit watermarking system, the condition of orthogonal watermarks again needs to be satisfied for multi-bit watermarking system. If using the KLT, this condition is available for the perfect reconstruction.

Then, the global correlation for extracting each bit b_k of the cooperative watermarking system as shown in (35).

$$r_{ck} = \sum_{i=1}^{m} w_i.r_{ik} \tag{35}$$

IV. EXPERIMENTAL RESULTS

As mentioned above, the smaller the block size is, the more embedded information capacity obtains. However, this leads to the shorter watermark length, which causes worse effects to the orthogonal condition and the host image interference. Therefore, we first examine the effects of the watermarks in practice.

Fig. 5 presents the results of similarity between different watermarks according to the watermark length by statistics of the maximum value and variance of correlation values of each pair of different watermarks for 20000 times. It shows that if the watermark length is small than 1000, the orthogonal condition is significantly violated by the limitation of the PRN generator.

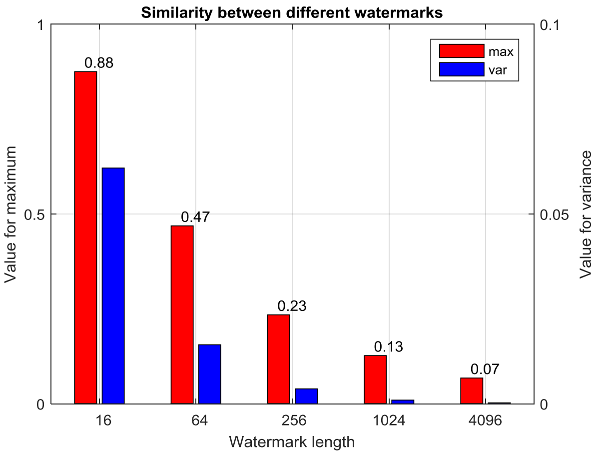

Figure 5. Similarity between different watermarks.

Table III presents the results of the interference between different image types (including natural and medical images) and 200 different watermarks with the same size as that of images. For each type of simulated images, the mean, maximum value and variance of the interference values are recorded. From the results, it can be seen that although the mean of interference is approximately zero, there is still significant variance, which degrades the performance of watermarking system. In addition, the interference also depends on the characteristics of each image type.

TABLE III. INTERFERENCE BETWEEN DIFFERENT IMAGE TYPES AND THE WATERMARK

Image	Size	Mean	Max	Var
Lena	512 x 512	0.0195	0.7542	0.0712
CT	640 x 599	-0.0094	0.2447	0.0116
MR	600 x 600	0.0039	0.4236	0.0234
US	900 x 600	0.0135	0.2534	0.0137
XR	640 x 599	-0.0131	0.4308	0.0346

For an example, Fig. 6 shows the mean square error (MSE) between the original KLT and the reconstructed KLT by simulation with the unique watermark and the orthogonal watermarks. It is clear that in the case of using the orthogonal watermarks, the error between the original KLT and the reconstructed KLT is close to zero due to the limitation of the PRN generator as mentioned above. However, the MSE increases significantly in the case of embedding the same watermark for all channels, especially with the high watermark energy. This is entirely consistent with theoretical analysis.

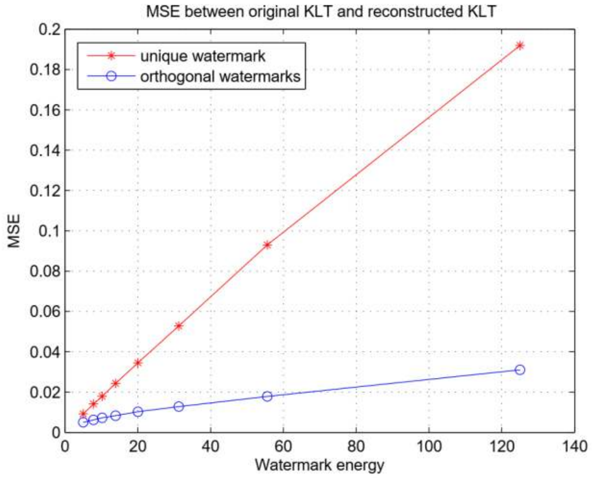

Figure 6. MSE between original KLT and reconstructed KLT.

Next, we investigate the results of theoretical analysis in Table I. Fig. 7 shows the comparison of error probability of the optimal and average (uniform) cooperative detectors for different selections of the watermark strength. In the first case, the watermark strength is uniform for each channel. It is selected in proportion to the variance of the local correlation in the second case and in proportion to the standard deviation of the local correlation in the third case. The distortion is fixed for all cases. It can be seen that the error probability of the optimal detector is always less than that of the average detector. In addition, the performance of the optimal detector with the proportional watermark strength is the same as that of the average detector with uniform watermark strength. Besides, the better performance is obtained with the equal watermark strength for each channel than watermark strength in proportion to the variance or the standard deviation of the local correlation. Therefore, the equal watermark strength is the best solution for both average and optimal detectors when the degradation of the watermarked images is only measured by MSE metric.

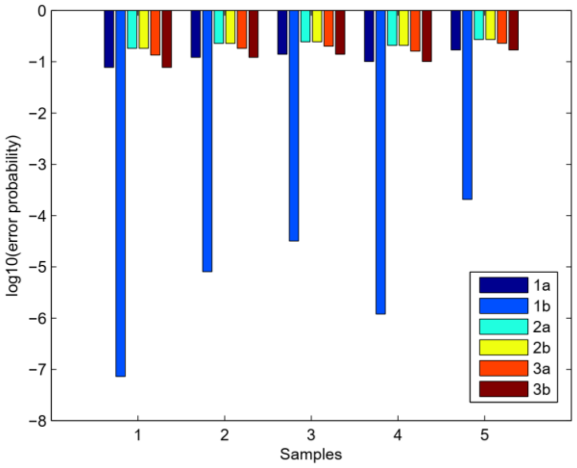

Figure 7. Comparison of error probability of the average (a) and optimal (b) detectors with respect to different selections of the watermark strengths.

Fig. 8 shows the error probability of the proposed watermarking system as a function of watermark energy without attack. It can be seen that the performance of the proposed watermarking system improves significantly when the number of channels increases. This corresponds to the theory.

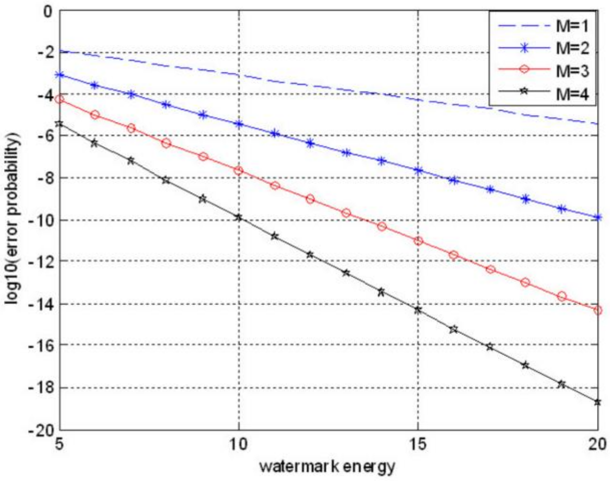

Figure 8. Error probability as a function of watermark energy without attack (different channel number).

Fig. 9 shows the error probability of the proposed watermarking system as a function of watermark energy with additive Gaussian noise in the case of two channels. As we can see, both results for simulation (points) and theory (curves) are likely identical, which means that the simulation results are similar to what are obtained in the theory. This figure also indicates that the performance of the proposed watermarking system improves significantly when the weighting vector is optimal. This again fits with theoretical analysis.

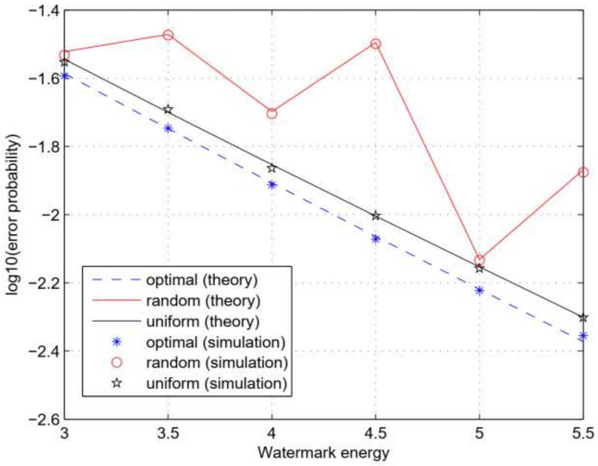

Figure 9. Error probability as a function of watermark energy with additive Gaussian noise (2 channels).

Fig. 10 shows the error probability of the proposed watermarking system without attack as a function of watermark energy in the case of three channels using the KLT. The energy ratio among Eigen-images equals to 50:10:1. It is clear that using the average weighting coefficients is not efficient in this case whereas the performance of the proposed watermarking system improves significantly with optimal weighting vector.

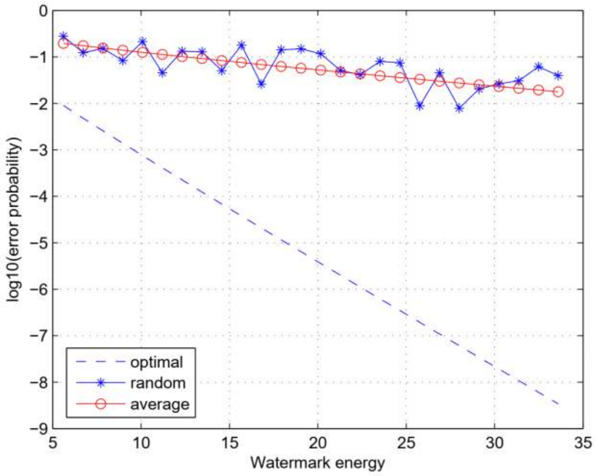

Figure 10. Error probability as a function of watermark energy without attack, and KLT Eigen-images energy ratio of 50:10:1.

V. CONCLUSION

In this paper, a new cooperative spread spectrum based blind watermarking technique for multi-channel images is proposed and analyzed. By utilizing a linear weighting vector in the extracting process, the optimal solution to minimize the error probability can be obtained. This proposed technique can be implemented in spatial domain or any other transform domain. Especially, with selection of the orthogonal watermarks, the KLT can be exploited to improve the performance of the watermarking system without the host images in the receiver. Moreover, the improved method to eliminate the interference between the host images and the watermark is also mentioned. Furthermore, the extensive methods to multi-bit watermarking are also discussed. The combination of these solutions can lead to a significantly efficient blind image watermarking system in security, capacity, invisibility and robustness. Finally, the experimental results are entirely consistent with theoretical analysis.

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 discussed the results; all authors had approved the final version.

ACKNOWLEDGMENT

This research is funded by Ho Chi Minh City University of Technology (HCMUT) - Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number T-DDT-2019-28.

REFERENCES

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

[2] N. Nikolaidis and I. Pitas, “Robust image watermarking in the spatial domain,” *IEEE Trans. Signal Processing*, vol. 66, no. 3, pp. 385-403, 1998.

[3] Y. Zhang and G. Sun, “A watermark algorithm based on space-domain and transform-domain,” in *Proc. International Conference on Electronics Information and Emergency Communication*, 2019, pp. 41-44.

[4] V. Chaudhary, A. Mishra, R. Mehta, M. Verma, R. P. Singh, and N. Rajpal, “Watermarking of grayscale images in DCT domain using least-squares support vector regression,” *International Journal of Machine Learning and Computing,* vol. 2, no. 6, pp. 725-728, 2012.

[5] L. Cai, H. Zhao, J. Cai, and L. Zhu, “A 3-D video watermark embedding technology in DCT-CS domain,” *International Journal of Machine Learning and Computing*, vol. 5, no. 3, pp. 206-213, 2015.

[6] P. F. Luis and P. G. Fernando, “Spread-Spectrum watermarking security,” *IEEE Trans. Information Forensics and Security*, vol. 4, no. 1, pp. 2-24, 2009.

[7] U. E. Peter, U. Parampalli, C. I. Uchechi, and O. Nnaemeka, “Challenges and prospects of blind spread spectrum medical image watermarking,” in *Proc. International Conference on Electro-Technology for National Development*, 2017, pp. 10-18.

[8] S. Sharma, L. K. Vishwamitra, and A. K. Sharma, “Enhancing spread spectrum watermarking using compression and encryption for standard images,” in *Proc. International Conference on Energy, Communication, Data Analytics and Soft Computing*, 2017, pp. 1479-1484.

[9] A. B. Bose and S. P. Maity, “Spread spectrum watermark detection on degraded compressed sensing,” *IEEE Sensors Letters*, vol. 1, no. 5, pp. 1-4, 2017.

[10] Y. Xiang, I. Natgunanathan, D. Peng, G. Hua, and B. Liu, “Spread spectrum audio watermarking using multiple orthogonal PN sequences and variable embedding strengths and polarities,” *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 26, no. 3, pp. 529-539, 2017.

[11] Y. G. Wang, G. Zhu, S. Kwong, and Q. S. Yun, “A study on the security levels of spread-spectrum embedding schemes in the WOA framework,” *IEEE Transactions on Cybernetics*, vol. 48, no. 8, pp. 2307-2320, 2018.

[12] Y. Huang, H. Guan, B. Niu, and S. Zhang, “A spread-spectrum watermarking scheme with adaptive embedding strength and PSNR guarantee,” in *Proc. International Conference on Anti-counterfeiting, Security, and Identification*, 2018, pp. 82-87.

[13] H. F. Tafreshi, R. Shakeri, and T. Khattab, “Capacious spread spectrum watermarking utilizing hadamard matrix,” in *Proc. International Conference on Wireless Communications and Mobile Computing*, 2016, pp. 570-575.

[14] B. Kumar, S. B. Kumar, and D. S. Chauhan, “Wavelet based imperceptible medical image watermarking using spread-spectrum,” in *Proc. International Conference on Telecommunications and Signal Processing*, 2015, pp. 1-5.

[15] 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.

[16] 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.

[17] 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.

[18] M. Barni, F. Bartolini, and A. Piva, “Multichannel watermarking of color images,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, no. 3, pp. 142-156, 2002.

[19] M. A. Hajjaji, A. Albouchi, and A. Mtibaa, “Combining DWT/KLT for secure transfer of color images,” in *Proc. International Conference on Design & Test of Integrated Micro & Nano-Systems*, 2019.

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 170 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.