Vulnerability Attacks of SVD-Based Video Watermarking Scheme in an IoT Environment

HERI PRASETYO,1 CHIH-HSIEN HSIA,2 (Member, IEEE), AND CHIN-HUA LIU2

1Department of Informatics, Universitas Sebelas Maret (UNS), Surakarta 57126, Indonesia
2Department of Computer Science and Information Engineering, National Ilan University, Yilan City 206, Taiwan

Corresponding author: Chih-Hsien Hsia (chhsia625@gmail.com)

This work was supported by the Ministry of Science and Technology of Taiwan, under Grants MOST 107-2221-E-197-025-MY2 and MOST 108-2511-H-006-008.

ABSTRACT This study reviews the superiority and limitations of the Singular Value Decomposition (SVD)-based video watermarking scheme. First applies key frame selection to the video sequence to obtain an appropriate video frame for the purpose of watermark embedding in this paper. The Fibonacci-Lucas image transformation scrambles the grayscale watermark image before the embedding process. The former scheme satisfies the imperceptibility and robustness aspects. However, it can suffer from the False-Positive-Problem (FPP) in which a counterfeit watermark image can be easily reconstructed by a malicious attacker. This study presents a new technique for overcoming the FPP of the aforementioned scheme. The proposed method embeds the principal components of the watermark image rather than the Singular Value Matrix (SVM) into the host video. As results, the proposed methods yield promising results in terms of imperceptibility as well as robustness. At the same time, it solves the FPP. A theoretical analysis of embedded watermark information is also provided in this work. The theoretical analysis meets the experimental-based results in the SVD-based video watermarking scheme.

INDEX TERMS False-positive-problem, watermarking, principal components, Fibonacci-Lucas transform, vulnerability attack.

I. INTRODUCTION

The usage of multimedia data has grown enormously in recent years. One example of multimedia usage is multimedia data communication via computer networks, the internet, cloud service, as well as the Internet-of-Things (IoT) devices. Nowadays, multimedia data in the format of images and videos has become very popular because it contains more information compared to that of the traditional text-based data. The popularity of image and video usage is also driven by the advance of low-price storage devices and fast communication devices. Securing multimedia data in communication becomes a vital issue. Multimedia data often consists of confidential information or secret valued messages. Several attempts have been developed to protect multimedia data, such as digital image watermarking [1]–[19], secret sharing [20]–[22], etc. These aforementioned methods show promising results in securing multimedia data.

The Singular Value Decomposition (SVD)-based image/video watermarking schemes are examples of recent advances in digital watermarking for securing multimedia data over communication networks and the IoT environment. Most of the SVD-based watermarking schemes simply embed the Singular Value Matrix (SVM) of the watermark information [1]–[7], [9]–[16]. The other schemes directly hide the watermark image into the singular value of the host image [8], [20]. These two simple approaches induce the FPP. This problem leads the ambiguous situation in which a malicious attacker can obtain a counterfeit watermark image from any arbitrary image or video. This condition is very serious from the perspective of copyright and authorship protection. Anyone can claim an authorized multimedia data based on the counterfeit extracted watermark image.

This work aims to solve the FPP caused by embedding the SVM of the watermark image into the host or cover media. The proposed method inherits the effectiveness of the SVD-based video watermarking scheme in [13]. The main difference between the proposed method and former scheme [13] lies in the type of watermark information embedded into the host image. Ponni and Ramakrishnan [13] inserts the SVM of the watermark image into the host...
image, whereas the proposed method renders the principal components of the watermark image into the host image. With our method, secret watermark information is embedded into the video sequence by exploiting the key frame selection and Fibonacci-Lucas image scrambling method. The former scheme cannot suffer from the FPP because of the SVM embedding strategy. The proposed method overcomes the FPP in [13] by inserting the principal components of the watermark image into the host or cover media. This works well and achieves impressive results for satisfying the imperceptibility and robustness aspects that can be directly applied for securing the multimedia data communication via the IoT environment. Figure 1 illustrates the schematic diagram of proposed method implementation. There are two parties involved in the video watermarking scheme in the IoT environment, i.e., the real video owner and an attacker. In this scenario, the real owner of the video aims to store his own video in the owner server. Before transmitting this video to the owner server, the real owner first embeds his watermark logo into his video for authorization purposes. The watermarked video is then stored on the owner server. On another occasion, the real owner may retrieve his watermarked video from the server via the cloud service or another peripheral. In a normal situation, the real owner will successfully collect his video and watermark logo. On the other hand, a malicious attacker may steal the video from the real owner server via the cloud environment and store it in another device. The malicious attacker cannot easily claim to be the real owner of the video because he cannot show his counterfeit watermark logo. All of these situations are implemented using the proposed method presented in this work over the IoT environment. Thus, the proposed method is very useful in avoiding an ambiguous situation for copyright and ownership protection.

In most typical SVD-based image watermarking schemes, two different metrics are employed to measure the performance of the aforementioned methods. These two metrics are the Peak-Signal-to-Noise-Ratio (PSNR) and Normalized Correlation Coefficient (NCC). The PSNR examines the similarity between the original host image and watermarked image. The PSNR computation is formally defined as:

$$
\text{PSNR} (A, A_w) = 10 \log_{10} \frac{255^2}{\frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (A(x, y) - A_w(x, y))^2}
$$

where $A$ and $A_w$ denote the original host image and watermarked image, respectively. These two images are the same size $M \times N$. The symbol $(x, y)$ denotes the spatial coordinates of the image pixel over $x = 1, 2, \ldots, M$ and $y = 1, 2, \ldots, N$. The NCC evaluates the similarity between the original watermark image and its extracted version. Then, the NCC is formally defined as (2), as shown at the bottom of the next page, where $W$ and $W^*$ denote the original watermark image and extracted watermark image, respectively. The $\mu_W$ and $\mu_{W^*}$ are the mean value of $W$ and $W^*$, respectively. The symbol $(i,j)$ represents the spatial position of a pixel in an image, for $i = 1, 2, \ldots, M$ and $j = 1, 2, \ldots, N$. Higher values of PSNR and NCC indicate greater similarity between two investigated/measured images. Thus, the SVD-based image watermarking schemes should achieve a higher PSNR score for the watermarked image as well as a higher NCC value for extracted watermark image.

In the field of SVD-based video/image watermarking schemes, our key contributions can be highlighted as follows: 1) Pointing out the FPP of the former SVD-based video watermarking scheme. 2) Developing a simple method to solve the FPP in [13]. 3) Presenting a formal mathematical analysis of the FPP in terms of Squared Error (SE). 4) Proving the FPP based on theoretical analysis of the correlation coefficient. Based on our best knowledge, this is the first time theoretical analysis of the SVD-based video and image watermarking has been conducted. Thus, the other researchers may consider these analyses before developing their own SVD-based video and image watermarking scheme to avoid the FPP. Further, we offer strong evidence that embedding the principal components yields better performance compared to inserting the SVM in the SVD-based video/image watermarking scheme.

The rest of this study is organized as follows: In Section II, reviews the former SVD-based video watermarking scheme along with its minor limitations. The proposed method for overcoming the problem of the former scheme in Section III. Sections IV and V provide theoretical analyses of the former scheme and the proposed method. Section VI shows performance comparisons with other existing methods. Conclusions are given in Section VII.

II. FORMER SVD-BASED VIDEO WATERMARKING SCHEME

We briefly discuss the usability and slight limitations of this aforementioned SVD-based video watermarking. The limitations of the [13] are reported with the experimental findings and supported by theoretical analysis. Therefore, we indicate the problem and offer a simple solution for this aforementioned issue. This part starts with the formal definition of SVD on decomposing an arbitrary matrix. Let $A$ be an
Suppose the SVD operation decomposes the matrix $A$. Each entry of this matrix is the real-value, i.e., $A \in \mathbb{R}^{N \times M}$. The SVD operation on matrix $A$ produces three matrices indicated as:

$$ A \Rightarrow U \Sigma V^T \quad (3) $$

where $U$ and $V$ are two unitary matrices, referred to as the left and right singular matrix, respectively. These two matrices are denoted as $U \in \mathbb{R}^{N \times r}$ and $V \in \mathbb{R}^{M \times r}$, respectively. The symbols $r$ and $T$ denote the rank of matrix $A$ and transpose operator on the matrix, respectively. In this work, the symbols $\Rightarrow$ or $\leftarrow$ denote the right and left assignment operator, respectively. The other matrix is simply an orthogonal matrix, referred to as a SVM, in which its diagonal entry consists of the Eigen-value of matrix $A$. This SVM is denoted as $\Sigma \in \mathbb{R}^{r \times r}$, while each diagonal can be represented as $\Sigma = \text{diag} \{\sigma_1, \sigma_2, \ldots, \sigma_r\}$. The values of $\sigma_i$ for $i = 1, 2, \ldots, r$ represent the singular value composing and ordering in ascending manner as $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r \geq 0$.

The typical SVD-based image watermarking schemes exploit the effectiveness of SVD operation to hide specific watermark information into the host image. Most SVD-based image watermarking methods embed the SVM of the watermark image into the host image. The main goal of this method is to obtain a good extracted watermark image in the watermark extraction step. A small disturbance of the SVM induces a slight distortion in a reconstructed image. The effect of disturbance on the SVM can be explained as follows.

Suppose the SVD operation decomposes the matrix $A$ into three matrices $U$, $V$, and $\Sigma$. Some noises are then injected into the SVM $\Sigma$. This noise injection is specifically denoted as $\Sigma + \varepsilon$, where $\varepsilon$ is generated random noise. By applying the inverse SVD operation, we obtain the reconstructed matrix $\hat{A}$. This inverse process can be represented as $U \hat{\Sigma} V^T \Rightarrow \hat{A}$.

If the magnitude of noise is small enough, then the reconstructed matrix $\hat{A}$ is visually similar to that of the original matrix $A$, i.e., $\hat{A} \approx A$. Figure 2 demonstrates the effect of noise addition into the SVM. Figure 2 (a) is the Lena image used as $A$, whereas the Figs. 2 (b)-(c) are the reconstructed images $\hat{A}$ obtained by injecting the zero-mean white Gaussian noise $\varepsilon$ with Standard Deviation (SD) of 10 and 25, respectively. Herein, the noise is only added into the diagonal component of the SVM $\Sigma$, i.e., $\hat{\sigma_i} \leftarrow \sigma_i + \varepsilon$, to obtain reconstructed image $\hat{A}$. It implies $\hat{\Sigma} = \text{diag} \{\hat{\sigma}_1, \hat{\sigma}_2, \ldots, \hat{\sigma}_r\}$. As shown in these figures, a small disturbance in the SVM yields an inferior effect on the reconstructed image. The reconstructed image is visually identical to that of the original image.

Another experiment is conducted to examine the effect of noise disturbance on the SVM. All entries in the SVM are added with the noise denoted as $\Sigma = \Sigma + \varepsilon$. Figures 2 (d)-(f), show the reconstructed images $\hat{A}$ while all entries of the SVM $\Sigma$ are distorted with zero-mean white Gaussian noise $\varepsilon$ under the SD are 5, 15, and 25, respectively. Even though the quality of reconstructed image $\hat{A}$ is less than the original image, we can still recognize $\hat{A}$ as Lena image. This is the main reason most typical SVD-based image watermarking schemes simply embed the SVM into the host image. The extracted SVM is often distorted or different compared to the original one. In this case, the extracted SVM can be viewed as a distorted SVM with additive noise. If we simply multiply this extracted SVM with the left and right singular matrices, it obtains an almost visually identical watermark image. Therefore, we always obtain a perfect extracted watermark image. This benefit led to the huge success of SVD-based image watermarking schemes.

In other cases, the watermark information is often embedded into the SVM of the host image. In this strategy, a host image is first divided into several non-overlapping blocks. The SVD operation further decomposes each image block to obtain two unitary ($U$, $V$) and one singular value ($\Sigma$) matrices. The watermark information is simply added into the largest singular value of each block. This process can be assumed as the noise injection into the largest singular value, i.e., $\hat{\sigma}_1 = \sigma_1 + \varepsilon$. By performing the inverse

![FIGURE 2. Effect of injecting the noise into the SVM: (a) Lena image used as testing data. (b)-(c) Adding the noise into the diagonal entries of the SVM. (d)-(f) Spreading the noise into all entries of the SVM. (g)-(i) Adding noise to the largest singular value of image blocks.](image)

$$ \text{NCC}(W, W^*) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} [W(i,j) - \mu_W][W^*(i,j) - \mu_{W^*}]}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} [W(i,j) - \mu_W]^2} \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} [W^*(i,j) - \mu_{W^*}]^2}} \quad (2) $$

VOLUME 8, 2020

69921
SVD operation on each image block, we obtain the reconstructed image $A$. Figure 2 (g)-(h) are the reconstructed image $A$ while the largest singular values of each image block are distorted with zero-mean white Gaussian noise over SD are 5, 15, and 25, respectively. These figures show the reconstructed images are visually identical to that of the original Lena image. This usability motivates the proposed method to deliver secure SVD-based image watermarking. The proposed method renders the watermark information into the largest singular value of each host image block.

A. EMBEDDING THE WATERMARK INFORMATION INTO THE HOST IMAGE

This method embeds a specific watermark image in grayscale format into the video sequence. This video is further referred to as the host video or media cover. The host video sequence is first processed with the key frame selection to obtain the best and suitable part of video for the watermark embedding purpose. Therefore, the red channel of the selected video frame is acquired to embed the secret watermark information. Since the former scheme only needs the red channel, it can be regarded as the typical SVD-based image watermarking scheme. Thus, the selected red channel of the host video is then regarded as the host image.

The formal watermark embedding of the former scheme is described in detail as follows. Let $A$ be a host image of size $M \times N$, while $W$ denotes the watermark image of size $m \times n$. Herein, the image $A$ is the red channel of the selected video frame. In [13] embeds the SVM of $W$ into $A$ by incorporating the two dimensional Discrete Wavelet Transform (DWT) [23]–[25] and Fibonacci-Lucas image scrambling method. Prospective readers are suggested to refer to [13] for a detailed explanation of the Fibonacci-Lucas image scrambling method. The step-by-step watermark embedding procedure in [13] is then given as follows:

**Step E1:** Perform a one-level DWT operation on host image $A$ to yield several transformed subbands denoted as:

$$\mathcal{J} \{A\} \Rightarrow \{A_{LL}, A_{LH}, A_{HL}, A_{HH}\} \quad (4)$$

where $\mathcal{J} \{\cdot\}$ and $A_{\theta}$ denote the DWT operation and DWT transformed subbands, respectively. For $\theta = \{LL, LH, HL, HH\}$.

**Step E2:** Select the LH-band of the DWT transformed image to hide the watermark image as:

$$X_s \leftarrow A_{LH} \quad (5)$$

where $X_s$ denotes the selected image for the watermark embedding purpose.

**Step E3:** Apply the SVD operation to the selected image $X_s$. This process is defined as:

$$X_s \Rightarrow U_A \Sigma_A V_A^T \quad (6)$$

where $U_A$ and $V_A$ are two unitary matrices of $A$, and $\Sigma_A$ is the SVM.

**Step E4:** Perform the Fibonacci-Lucas image scramble on watermark image $W$. This scrambling process is defined as:

$$L \{W\} \Rightarrow W_b \quad (7)$$

where $L \{\cdot\}$ and $W_b$ denote the operator of Fibonacci-Lucas image scrambling and the scrambled watermark image, respectively.

**Step E5:** Apply the SVD operation to the scrambled watermark image $W_b$ as follows:

$$W_b \Rightarrow U_w \Sigma_w V_w^T \quad (8)$$

where $U_w$ and $V_w$ are two unitary matrices, and $\Sigma_w$ is the SVM.

**Step E6:** Embed the watermark information as contained in SVM $\Sigma_w$ into the SVM $\Sigma_A$ of the host image as:

$$\Sigma_n \leftarrow \Sigma_A + \alpha \Sigma_w \quad (9)$$

where $\Sigma_n$ and $\alpha$ denote the modified SVM of the host image and scaling factor, respectively. This part is the most critical step in typical SVD-based image watermarking.

**Step E7:** Apply the inverse SVD operation by multiplying three matrices $\Sigma_n$, $U_A$, and $V_A$. This process is represented as:

$$X_{sw} \leftarrow U_A \Sigma_n V_A^T \quad (10)$$

where $X_{sw}$ denotes the watermarked image in the LH-band. In this process, the matrices $U_A$ and $V_A$ are obtained from Step E6. Whereas, the matrix $\Sigma_n$ is from Step E5.

**Step E8:** Perform a one-level inverse DWT operation of the host subbands by replacing the LH-band with $X_{sw}$. This computation is defined as:

$$A_w \leftarrow \mathcal{J}^{-1} \{A_{LL}, X_{sw}, A_{HL}, A_{HH}\} \quad (11)$$

where $A_w$ and $\mathcal{J}^{-1} \{\cdot\}$ denote the watermarked image and operator of the inverse DWT process, respectively. The subbands $A_{LL}$, $A_{HL}$, and $A_{HH}$ are from Step E1. From this step, we obtain the watermarked image containing the watermark information.

B. EXTRACTING THE WATERMARK INFORMATION FROM THE WATERMARKED IMAGE

The watermark extraction process is substantially the reverse process of the watermarking embedding. The watermark information is retrieved from the watermarked process. In [13], the key frame selection is first applied to the watermarked video sequence. This process produces the selected frame of the watermarked video. Since the former scheme only considers the red channel of this selected frame, the watermark extraction process thus reduces to the typical SVD-based image watermark extraction.

We attempt to extract the watermark information from the watermarked image obtained after key frame selection and red channel determination. The subsequent processes for the extraction procedures are then given as follows. Let $A_w^*$ be the potentially corrupted the watermarked image. In most
situations, the watermarked image is often destroyed by some image manipulations or geometric distortions such as noise addition, cropping, etc. The watermark extraction process aims to reconstruct the watermark image from \( A_{w^*} \).

**Step X1:** Perform one-level DWT decomposition on \( A_{w^*} \) as:

\[
\mathcal{A} \{ A_{w^*} \} \leq \{ A_{LL}^*, A_{LH}^*, A_{HL}^*, A_{HH}^* \} \quad (12)
\]

where \( A_{s}^* \) denotes the transformed subbands, for \( \theta = \{ LL, LH, HL, HH \} \).

**Step X2:** Select the LH transformed image to retrieve the watermark image. It can be calculated as:

\[
X_s^* \leftarrow A_{LH}^* \quad (13)
\]

where \( X_s^* \) denotes the selected LH-band of a potentially corrupted watermarked image.

**Step X3:** Apply the SVD decomposition on \( X_s^* \) to obtain three matrices as defined below:

\[
X_s^* \Rightarrow U_A^* \Sigma_A^* V_A^T \quad (14)
\]

where \( U_A^* \), \( V_A^* \), and \( \Sigma_A^* \) are the decomposed matrices. We only need matrix \( \Sigma_A^* \) to extract the watermark image.

**Step X4:** Extract the SVM of the watermark image as:

\[
\Sigma_{w^*} \leftarrow \frac{1}{\alpha} (\Sigma_A^* - \Sigma_A) \quad (15)
\]

where \( \Sigma_{w^*} \) denotes the extracted SVM of the watermark image. Herein, the matrix \( \Sigma_A \) is from Step E3 of the watermark embedding process. The scaling factor \( \alpha \) should be identical to that used in Step E6 of the watermark embedding stage to yield the correct result.

**Step X5:** Reconstruct the watermark image using the inverse SVD operation as:

\[
W_b^* \leftarrow U_w^* \Sigma_w^* V_w^T \quad (16)
\]

where \( W_b^* \) denotes the extracted watermark image. It should be noted \( W_b^* \) is still in scrambled form. An additional step is required to obtain the final extracted watermark image. The matrices \( U_w^* \) and \( V_w^* \) for computing the \( W_b^* \) are obtained from Step E5 of the watermark embedding process. These two unitary matrices can be regarded as secret keys in the SVD-based image watermarking scheme.

**Step X6:** Apply the inverse Fibonacci-Lucas image scrambling method to \( W_b^* \) as:

\[
W^* \leftarrow \mathcal{L}^{-1}\left\{ W_b^* \right\} \quad (17)
\]

where \( W^* \) and \( \mathcal{L}^{-1}\{ \cdot \} \) denote the extracted watermark image and operator of the inverse Fibonacci-Lucas image scrambling, respectively. This descrambling operation forces each pixel on the extracted watermark image into the original position. Thus, we obtain an acceptable extracted watermark image.

**C. VULNERABILITY ATTACKS ON THE FORMER METHOD**

In [13], the SVD-based video watermarking scheme satisfies the imperceptibility and robustness aspects. The watermark image cannot be easily perceived in the watermarked image. Therefore, the watermark image can be successfully extracted from the watermarked image, even though this image is corrupted by some noise or destroyed by common manipulations and distortions. The following experiment reports the effectiveness of the [13]. Figure 3 shows several video clips for testing purposes. These videos in color format are regarded as the host video or cover media. A set of grayscale images in Fig. 4 are turned into the watermark image. In the first experiment, the watermark image in Fig. 4 (a) is embedded into the host video in Fig. 3 (a) by selecting the scaling factor \( \alpha = 0.1 \). Herein, the watermark image is first scrambled with the Fibonacci-Lucas transform using the specific secret key \( X_1 \). Figure 5 (a) displays the watermarked image yielding PSNR = 35.03 dB. Based on this result, the former SVD-based video watermarking scheme satisfies the imperceptibility aspect indicating a high PSNR value. The watermark image which is directly extracted from the watermarked image, as shown in Fig. 5 (b). It produces NCC = -0.0017. After performing the inverse Fibonacci-Lucas transform with secret key \( X_1 \), the extracted watermark image is given in Fig. 5 (c). The NCC value of this watermark image is NCC = 0.9949. Again, the former scheme yields a good extracted watermark image with a high NCC score. Figure 5 (d) shows the extracted watermark image after applying the inverse Fibonacci-Lucas transform with different secret key \( X_2 \). It induces the NCC = -0.0021 for the extracted watermark image. The additional step in the watermarking scheme, i.e. Fibonacci-Lucas transform, increases the robustness aspect of the high security issue. Thus, the former SVD-based video watermarking scheme yields good results in terms of imperceptibility and high security aspects.
Additional experiments are conducted to test the robustness aspect of the former SVD-based video watermarking scheme. Herein, the watermarked image is manipulated by injecting noises, cropping, etc. Figure 6 depicts a set of watermarked images after applying several malicious attacks such as: (a) JPEG compression with $Q = 80$, (b) Gaussian noise with $\sigma = 10^{-3}$, (c) Multiplicative uniform noise with $\sigma = 5 \times 10^{-3}$, (d) Additive uniform noise with $p = 5 \times 10^{-3}$, (e) Salt and pepper noise with $p = 10^{-2}$, (f) Mean filter with kernel size $3 \times 3$, (g) Gamma correction with $\gamma = 98 \times 10^{-2}$, (h) Laplacian image unsharpening, (i) Image rescaling from $512 \times 512$ to $256 \times 256$ and back to $512 \times 512$, (j) Median filtering with kernel size $3 \times 3$, (k) Speckle noise with $p = 10^{-3}$, and (l) Adding all pixels with value 10. Figure 7 shows a set of extracted watermark images after extracting the watermark information from a set of attacked watermarked images in Fig. 6. These attacks are quite similar to the typical SVD-based image watermarking scheme because the [13] applies the key frame selection on the host video to embed the watermark information. The key frame selection in the host video produces the selected area which is in two dimensional data or image format. Thus, the host data can be regarded as an image. This situation offers an easy way to embed the watermark information in image format into the host data (in the two dimensional image). Therefore, the watermark insertion and extraction in [13] can be applied accordingly. In this experiment, we use the correct key for the Fibonacci-Lucas image scrambling that the NCC scores of Fig. 7 are respectively reported as:

$$\text{NCC} = \{0.9857, 0.9792, 0.9843, 0.9914, 0.9637, -0.9636, 0.9953, 0.9909, -0.9436, 0.6519, 0.9890, 0.9932\}.$$ 

From this experiment, it can be concluded the former scheme is robust against malicious attacks, i.e. common image manipulations and geometric distortions.

The other experiment examines the FPP in the former SVD-based video watermarking scheme. This problem causes the vulnerability attack on the SVD-based video/image watermarking scheme. This vulnerability attack occurs while an unauthorized attacker tries to generate the counterfeit watermark image from any arbitrary watermark image. In this situation, an attacker can successfully obtain the counterfeit watermark image and claim authorship. The vulnerability attack can be illustrated as follows. Suppose an attacker tries to extract the watermark image from the watermarked image as given in Fig. 5 (a). In this case, we know the watermarked image of Fig. 5 (a) contains the watermark image of Fig. 4 (a). This attacker directly extracts the watermark information using the wrong side information, i.e. $U_w$ and $V_w$ obtained from Fig. 4 (b)-(d). Herein, a set of Fig. 4 (b)-(d) are referred to as the counterfeit watermark image. In Fig. 8 (a), (c), and (e) are extracted watermark images, respectively with NCC $\{0.0016, -0.0044, 0.0026\}$, obtained using the wrong side information from Fig. 4 (b)-(d). After applying the Fibonacci-Lucas transformation with the correct key, the extracted watermark images can be seen in Fig. 8 (b), (d), and (f). The NCC values of these extracted watermark images are respectively $\{0.9918, 0.9689, 0.9953\}$. The extracted watermark images...
A PROPOSED WATERMARK EMBEDDING STRATEGY

In contrast to the [13], the proposed method embeds the principal components of the watermark image into the host video. The principal components are the matrix obtained from the multiplication between the left singular vector and SVM. The usage of the principal component effectively overcomes the FPP. In similar fashion to that of [13], the proposed method employs key frame selection to acquire the best and suitable video sequence for injecting the watermark information. Only the red channel is needed on the selected frame. Therefore, the proposed method can also be considered a typical SVD-based image watermarking scheme.

The proposed method requires a host image $A$ of size $M \times N$ and watermark image $W$ of size $m \times n$ that the method embeds $W$ into $A$ with the block-wise strategy, i.e., one piece of watermark image information is embedded into one image block of the host image. The proposed method also needs the DWT and SVD in the watermark embedding and extraction process. Thus, the proposed watermark embedding can be explained step-by-step as follows:

**Step WE-1:** Perform one-level DWT operation on host image $A$ as:

$$L\{A\} \Rightarrow \{A_{LL}, A_{LH}, A_{HL}, A_{HH}\}$$ (18)

**Step WE-2:** Select the LL-band of the DWT transformed host image. The selected subband is further divided into several non-overlapping blocks denoted as:

$$A_{LL} \Rightarrow \{a_1, a_2, \ldots, a_i, \ldots, a_{\frac{MN}{mn}}\}$$ (19)

where $a_i$ denotes the $i$-th image block of LL-band, for $i = 1, 2, \ldots, \frac{MN}{mn}$. Herein, the number of image blocks should be identical to the number of pixels on the watermark image.

**Step WE-3:** Perform the Fibonacci-Lucas image scrambling on the watermark image as:

$$L\{W\} \Rightarrow W_b$$ (20)

where $W_b$ denotes the scrambled watermark image.

**Step WE-4:** Apply the SVD operation to the scrambled watermark image $W_b$ as follows:

$$W_b \Rightarrow U_w \Sigma_w V_w^T$$ (21)

**Step WE-5:** Compute the principal components of the watermark image as:

$$W_{U \Sigma} \Leftarrow U_w \Sigma_w$$ (22)

where $W_{U \Sigma}$ denotes the principal components of the watermark image. Herein, the size of $W_{U \Sigma}$ is also $m \times n$. In contrast with the [13], the proposed method embeds the principal components into the host image.

**Step WE-6:** Apply the SVD operation to each image block $a_i$ that the decomposition process can be denoted as:

$$a_i \Rightarrow U_i \Sigma_i V_i^T$$ (23)

where $U_i$, $V_i$, and $\Sigma_i$ are three matrices of image block $a_i$. Herein, we apply the SVD operation over all image blocks, for $a_i$ and $i = 1, 2, \ldots, \frac{MN}{mn}$. The diagonal component of matrix $\Sigma_i$ is $\Sigma_i = \text{diag}(\sigma_1, \sigma_2, \ldots, \sigma_f, 0, \ldots, 0)$. We only consider the largest singular value, i.e., $\sigma_1$, for the watermark embedding purpose.

**Step WE-7:** Embed the principal components of the watermark image into the largest singular value of each image block as:

$$\lambda_{w}(x, y) \Leftarrow \sigma_1 + a W_{U \Sigma}(x, y)$$ (24)

where $\lambda_w(x, y)$ denotes the modified largest singular value. The value of $W_{U \Sigma}(x, y)$ indicates the principal component of the watermark image on position $(x, y)$, for $x = 1, 2, \ldots, m$ and $y = 1, 2, \ldots, n$. Similar to the [13], this step is the most critical point in the proposed watermark embedding process.
**Step WE-8:** Replace the largest singular value ($\sigma_1$) of each image block $a_i$ with the value of $\lambda_w(x, y)$. This replacement process can be performed as:

$$\Sigma_{iw} \leftarrow \text{diag}(\lambda_w(x, y), \sigma_2, \ldots, \sigma_r, 0, \ldots, 0)$$  \hspace{1cm} (25)

where $\Sigma_{iw}$ denotes the modified SVM on the $i$-th image block, for $i = 1, 2, \ldots, \frac{MN}{2mn}$. The matrices $U_i$ and $V_i$ are obtained from Step WE-6.

**Step WE-9:** Collect all modified image blocks, $a_{iw}$, and construct a modified LH-band. This process can be given as follows:

$$A_{LL}^w \leftarrow \left\{ a_{1w}, a_{2w}, \ldots, a_{iw}, \ldots, a_{w} \right\}_{\frac{MN}{2mn}}$$  \hspace{1cm} (27)

where $A_{LL}^w$ is the modified LL-band.

**Step WE-10:** Perform inverse one-level DWT operation to obtain a watermarked image as:

$$A_w \leftarrow \mathcal{J}^{-1} \left\{ A_{LL}^w, A_{LH}, A_{HL}, A_{HH} \right\}$$  \hspace{1cm} (28)

where $A_w$ denotes the watermarked image.

**B. PROPOSED WATERMARK EXTRACTION STRATEGY**

The watermark extraction process of the proposed method can be simply performed over several steps. The key frame selection and red channel determination are applied to the watermarked video sequence to obtain a specific watermark image. The watermark extraction process of the proposed method is explained as follows. Let $A_{w}^*$ be the potentially corrupted watermark image. The following steps are conducted for extracting the watermark image from $A_{w}^*$:

**Step WX-1:** Perform one-level DWT operation on image $A_{w}^*$ as:

$$\mathcal{J} \left\{ A_{w}^* \right\} \Rightarrow \left\{ A_{LL}^*, A_{LH}^*, A_{HL}^*, A_{HH}^* \right\}$$  \hspace{1cm} (29)

where $A_{\theta}^*$ denotes the transformed subbands, for $\theta = \{LL, LH, HL, HH\}$.

**Step WX-2:** Select the LL-band and divide it into several non-overlapping image blocks. The size of the image block should be identical to that used in the watermark embedding process as:

$$A_{LL}^* \Rightarrow \left\{ a_1^*, a_2^*, \ldots, a_i^*, \ldots, a_{\frac{MN}{2mn}}^* \right\}$$  \hspace{1cm} (30)

where $a_i^*$ denotes the $i$-th image block of transformed LL-band, for $i = 1, 2, \ldots, \frac{MN}{2mn}$.

**Step WX-3:** Decompose each image block $a_i^*$ using the SVD operation as:

$$a_i^* \Rightarrow U_i^* \Sigma_i^* V_i^{*T}$$  \hspace{1cm} (31)

where $U_i^*$, $\Sigma_i^*$, and $V_i^*$ are three SVD matrices obtained from the $i$-th image block, for $i = 1, 2, \ldots, \frac{MN}{2mn}$. Herein, the SVM can be defined as $\Sigma_i^* \leftarrow \text{diag}(\sigma_1^*, \sigma_2^*, \ldots, \sigma_r^*, 0, \ldots, 0)$. For each image block, we only consider the largest singular value, i.e. $\sigma_1^*$, for the subsequent watermark extraction process.

**Step WX-4:** Extract the principal component of the watermark image from the largest singular value $\sigma_1^*$ of each image block. This extraction process can be computed as follows:

$$W^*_u(x, y) \leftarrow \frac{1}{\alpha} (\sigma_1^* - \sigma_1)$$  \hspace{1cm} (32)

where $W^*_u(x, y)$ denotes the extracted principal component on pixel position $(x, y)$, for $x = 1, 2, \ldots, m$ and $y = 1, 2, \ldots, n$. The value of $\sigma_1$ is from Step WE-7 under the same position $(x, y)$.

**Step WX-5:** Reconstruct the watermark image by multiplying the extracted principal component $W^*_u$ with $V_w$ that can be calculated as follows:

$$W^*_b \leftarrow W^*_u V_w^T$$  \hspace{1cm} (33)

where $W^*_b$ denotes the reconstructed extracted watermark image. Herein, the matrix $V_w$ is obtained from Step WE-4. The matrix $V_w$ can be regarded as a secret key in the proposed SVD-based image/video watermark method.

**Step WE-6:** Apply the inverse Fibonacci-Lucas image scrambling to image $W^*_b$. This image descrambling process can be defined as:

$$W^* \leftarrow \mathcal{L}^{-1} \left\{ W^*_b \right\}$$  \hspace{1cm} (34)

where $W^*$ denotes the extracted watermark image. Herein, the secret key for Fibonacci-Lucas image scrambling should be identical to the watermark embedding and extraction process.

**C. PROPOSED METHOD WITH ADAPTIVE SCALING FACTOR**

The scaling factor plays an important role in the SVD-based image/video watermarking schemes. The scaling factor, $\alpha$, determines the robustness strength as well as the imperceptibility aspects. A suitable $\alpha$ value effectively hides the watermark image such that its presence cannot be perceived by human vision. It can be said the SVD-based image and video watermarking methods satisfy the imperceptibility criterion for good algorithm design. In addition, the developing watermarking methods with specific $\alpha$ should be robust against several image manipulations and geometric distortions that can be regarded as malicious attacks. A good watermarking scheme should meet the robustness issue against several unauthorized malicious attacks.

The determination of $\alpha$ is not easy task. The presence of the watermark image cannot be perceived by setting a small $\alpha$ value. However, it is less robust against several malicious attacks with small $\alpha$. In contrast, the SVD-based image/video watermarking becomes more robust against various attacks by incorporating a high value $\alpha$. Therefore, the watermark image will be easily recognized in the watermarked image.
with high $\alpha$. In addition, choosing a single scaling factor is less suitable for the SVD-based image/video watermarking scheme in adapting to hard malicious attacks [19]. Despite using a single scaling factor, in [13] employs an adaptive scaling factor. This strategy gives different scaling factors by examining the magnitude of the watermark information. The adaptive scaling factor can be viewed as constructing $\alpha$ in matrix form rather than a single value that the factor $\alpha$ of size $N \times M$ is formally defined as follows:

$$a_{i} = \alpha_{\text{min}} - \frac{i}{N} (\alpha_{\text{min}} - \alpha_{\text{max}}) \quad (35)$$

For $i = 1, 2, \ldots, N$, where $\alpha_{\text{min}}$ and $\alpha_{\text{max}}$ are the minimum and maximum limit of the factor. These two values are commonly set as $\alpha_{\text{min}} = 0.25$ and $\alpha_{\text{max}} = 1$ [19]. Herein, the symbol $j$ denotes the row of watermark images. Different rows of watermark images own different scaling factors. Thus, the robustness and imperceptibility will increase using the adaptive scaling factor.

IV. THEORETICAL ANALYSIS IN TERMS OF SQUARED-ERROR

This section delivers the theoretical analysis between the proposed method and [13] in terms of SE. The problem of the former scheme is explained in detail in this section and supported by theoretical analysis. Therefore, the benefit and correctness of the proposed method are also given in this section. Thus, we can expect an objective measurement between the proposed method and former scheme. This section starts with discussion of SE and PSNR. The effects of embedding the SVM and principal components are then analyzed with formal mathematics to illustrate the occurrence of the FPP.

A. SQUARE-ERROR AND PEAK-SIGNAL-TO-NOISE-RATIOS

The value of SE is simply the norm of difference between two compared matrices/images. This value can be computed as:

$$\text{SE}(A_1, A_2) = \|A_1 - A_2\|_2^2 \quad (36)$$

where $\|\cdot\|_2$ denotes the Euclidean norm. Therefore, the Euclidean norm of difference between $A_1$ and $A_2$ is given as $\|A_1 - A_2\|_2^2 = \sum_{i=1}^{M} \sum_{j=1}^{N} (A_1(x, y) - A_2(x, y))^2$. The symbols $M$ and $N$ denote the image size. The SE score between the two images can be simply calculated from the sum of the squared difference between each pixel of two measured matrices/images. Thus, the PSNR value can be also defined in terms of SE as follows:

$$\text{PSNR}(A_1, A_2) = 10 \log_{10} \left( \frac{255^2}{\text{SE}(A_1, A_2)} \right) \quad (37)$$

where $\|A_1 - A_2\|_2^2$ denotes the SE between $A_1$ and $A_2$. This PSNR computation is identical to that of the PSNR calculation in (1). If $A_1$ and $A_2$ are diagonal matrices, the PSNR calculation in (37) implies a simpler computation compared to that used in (1). The SE in (37) can be only calculated over diagonal entries between $A_1$ and $A_2$, not in element-wise computation as used in (1).

B. EFFECT OF EMBEDDING A SINGULAR VALUE

This subsection presents the effect of embedding a singular value into the host image used in [13]. This technique induces the FPP. The formal analysis is given as follows. Let $W$ and $W^*$ be the original watermark image and extracted watermark image, respectively. These two matrices employ two identical matrices, $U_w$ and $V_w$. The only difference between $W$ and $W^*$ lies in their SVM. In the watermark embedding step [13], the SVD decomposes $W$ to yield three matrices $U_w$, $\Sigma_w$, and $V_w$, as indicated by the following process:

$$W = U_w \Sigma_w V_w^T \quad (38)$$

The matrices $U_w$ and $V_w$ are secretly kept as secret keys for the watermark extraction purpose. Some malicious attacks or rounding operations after the watermark embedding process may destroy the quality of the watermarked image. Thus, the extracted watermark image cannot be perfectly obtained in the extraction process. Let $\Sigma^*_w$ be the extracted SVM obtained from the potentially corrupted watermarked image. Then, the extracted watermark image $W^*$ can reconstruct by multiplying the extracted SVM $\Sigma^*_w$ with secret keys $U_w$ and $V_w$ as indicated below:

$$W^* = U_w \Sigma^*_w V_w^T \quad (39)$$

The similarity between $W$ and $W^*$ can be assessed in terms of SE between these two matrices with the element-wise composition as formulated:

$$\|W - W^*\|_2^2 = \sum_{x=1}^{M} \sum_{y=1}^{N} (W(x, y) - W^*(x, y))^2 \quad (40)$$

By substituting (38) and (39) into (40), the SE between $W$ and $W^*$ can be further redefined as:

$$\|W - W^*\|_2^2 = \sum_{x=1}^{M} \sum_{y=1}^{N} \left( U_w \Sigma_w V_w^T - U_w \Sigma^*_w V_w^T \right)^2 \quad \Rightarrow \quad \|W - W^*\|_2^2 \leq \|U_w \Sigma_w V_w^T - U_w \Sigma^*_w V_w^T\|_2^2 \quad (41)$$

where $\{\cdot\}$ denotes the trace of the matrix operator. With simple matrix algebraic manipulation, the last form can be further simplified as

$$\text{Tr} \left\{ \left( U_w \Sigma_w V_w^T - U_w \Sigma^*_w V_w^T \right)^T \left( U_w \Sigma_w V_w^T - U_w \Sigma^*_w V_w^T \right) \right\}$$

$$\text{Tr} \left\{ \left( U_w \Sigma_w V_w^T - U_w \Sigma^*_w V_w^T \right)^T U_w \Sigma_w V_w^T + \left( U_w \Sigma_w V_w^T - U_w \Sigma^*_w V_w^T \right) U_w \Sigma^*_w V_w^T - \left( U_w \Sigma^*_w V_w^T \right)^T U_w \Sigma^*_w V_w^T - U_w \Sigma^*_w V_w^T U_w \Sigma^*_w V_w^T \right\} \quad (42)$$

H. Prasetyo et al.: Vulnerability Attacks of SVD-Based Video Watermarking Scheme in an IoT Environment
Since $U_w$ is the unitary matrix, it implies $U_w^T U_w = I$. The property of identity matrix tells us $AI = IA = A$. Thus, the SE in (42) can be subsequently simplified as

$$
\begin{align*}
&\text{Tr} \left\{ V_w \Sigma_w^T \Sigma_w V_w^T - V_w \Sigma_w^T \Sigma_w^* V_w^T - V_w \Sigma_w^* \Sigma_w V_w^T \right\} \\
&+ V_w \Sigma_w^* \Sigma_w^* V_w^T \\
= &\text{Tr} \left\{ V_w \Sigma_w^T \Sigma_w V_w^T - V_w \Sigma_w^T \Sigma_w^* V_w^T - V_w \Sigma_w^* \Sigma_w V_w^T \right\} \\
&+ V_w \Sigma_w^* \Sigma_w^* V_w^T
\end{align*}
$$

(43)

By incorporating the unitary property of $V_w$, i.e. $V_w V_w^T = V_w^T V_w = I$, each entry in (43) can be simply as below:

$$
\begin{align*}
V_w \Sigma_w^T \Sigma_w V_w^T &= V_w V_w^T \Sigma_w = \Sigma_w \\
V_w \Sigma_w^T \Sigma_w^* V_w^T &= V_w V_w^T \Sigma_w^* = \Sigma_w^* \\
V_w \Sigma_w^* \Sigma_w V_w^T &= V_w V_w^T \Sigma_w = \Sigma_w \\
V_w \Sigma_w^* \Sigma_w^* V_w^T &= V_w V_w^T \Sigma_w^* = \Sigma_w^*
\end{align*}
$$

(44) - (47)

Substituting (44) to (47) into (43), one can trivially obtain:

$$
\begin{align*}
&\text{Tr} \left\{ \Sigma_w^T \Sigma_w - \Sigma_w^T \Sigma_w^* - \Sigma_w^* \Sigma_w + \Sigma_w^T \Sigma_w^* \right\} \\
= &\text{Tr} \left\{ \Sigma_w^T \Sigma_w - 2 \Sigma_w^T \Sigma_w^* + \Sigma_w^* \Sigma_w^* \right\}
\end{align*}
$$

(48)

The SVM consists of non-zero entries in the diagonal element. Therefore, the two entries in (48) are equivalent as summation between their diagonal element indicated as $\Sigma_w^T \Sigma_w^* = \sum_{i=1}^r \sigma_w^r(r) \sigma_w^r(r)$ and $\Sigma_w^* \Sigma_w = \sum_{i=1}^r \sigma_w^r(r) \sigma_w (r)$. This implies $\Sigma_w^T \Sigma_w^* = \Sigma_w^* \Sigma_w$. Subsequently, the form (48) can be further recalculated as

$$
\begin{align*}
&\text{Tr} \left\{ \Sigma_w^T \Sigma_w - \Sigma_w^T \Sigma_w^* - \Sigma_w^* \Sigma_w + \Sigma_w^T \Sigma_w^* \right\} \\
= &\text{Tr} \left\{ \Sigma_w^T \Sigma_w - 2 \Sigma_w^T \Sigma_w^* + \Sigma_w^* \Sigma_w^* \right\}
\end{align*}
$$

(49)

Using the definition of matrix trace, the form in (49) is then given as $\text{Tr} \left\{ \left( \Sigma_w - \Sigma_w^* \right)^T \left( \Sigma_w - \Sigma_w^* \right) \right\}$. Finally, one obtains the final form as $\| \Sigma_w - \Sigma_w^* \|^2_2$. The last form indicates the SE between $W$ and $W^*$ is equivalent to:

$$
\| W - W^* \|^2_2 = \left\| U_w \Sigma_w V_w^T - U_w \Sigma_w^* V_w^T \right\|^2_2 = \left\| \Sigma_w - \Sigma_w^* \right\|^2_2
$$

(50)

The SE between the original and extracted watermark is equivalent to the SE between their singular value matrices if they incorporate identical $U_w$ and $V_w$.

The PSNR score between the original watermark image $W$ and extracted watermark image $W^*$ can be computed as:

$$
\text{PSNR} (W, W^*) = 10 \log_{10} \frac{255^2}{\frac{1}{MN} \left\| W - W^* \right\|^2_2}
$$

(51)

where $\| W - W^* \|^2_2$ denotes the SE between $W$ and $W^*$. Since $\| W - W^* \|^2_2 = \| \Sigma_w - \Sigma_w^* \|^2_2$, the PSNR computation in (51) can be also defined as:

$$
\text{PSNR}(\Sigma_w, \Sigma_w^*) = 10 \log_{10} \frac{255^2}{\frac{1}{MN} \left\| \Sigma_w - \Sigma_w^* \right\|^2_2}
$$

(52)
C. EFFECT OF EMBEDDING PRINCIPAL COMPONENTS

This subsection describes the effect of embedding the principal components into the host image. The usage of principal components in the proposed method effectively overcomes the FPP. The detailed formal mathematical analysis of embedding principal components for the proposed method is given as follows. Let \( W \) and \( W^* \) be the original watermark image and extracted watermark image, respectively. First, the SVD decomposes \( W \) to yield three matrices as:

\[
W = U_w \Sigma_w V_w^T
\]

(53)

Then, the \( W^* \) is composed by multiplication of its principal components, i.e., \( U_w^* \Sigma_w^* \), with the left singular vector \( V_w \) of \( W \). This process is illustrated as:

\[
W^* \leftarrow U_w^* \Sigma_w^* V_w^T
\]

(54)

Performing the matrix algebra, the value of \( \| W - W^* \|_2^2 \) is subsequently simplified as

\[
\begin{align*}
&\text{Tr} \left\{ (U_w \Sigma_w V_w^T - (U_w \Sigma_w^*) V_w^T)^T (U_w \Sigma_w^* V_w^T) \\
&- (U_w \Sigma_w^* V_w^T)^T (U_w \Sigma_w V_w^T) + (U_w^* \Sigma_w^* V_w^T)^T (U_w^* \Sigma_w^* V_w^T) \right\}.
\end{align*}
\]

(56)

Based on the unitary property of SVD resulted matrix, it yields two conclusions, i.e., \( U_w^T U_w = I \) and \( V_w V_w^T = I \). The first term in (56) can be simplified as:

\[
V_w \Sigma_w^T U_w^T U_w \Sigma_w V_w^T = V_w \Sigma_w^T I \Sigma_w V_w^T = V_w \Sigma_w^T \Sigma_w V_w^T = \Sigma_w I \Sigma_w = \Sigma_w^2
\]

(57)

The second term in (56) is also described as:

\[
V_w \Sigma_w^* U_w^T U_w^* \Sigma_w^* V_w^T = \Sigma_w^* U_w^T U_w^* \Sigma_w^* V_w^T = \Sigma_w^* U_w^T U_w^* \Sigma_w^* V_w^T
\]

(58)

The third term in (57) is equivalent to \( V_w \Sigma_w^T U_w^T U_w \Sigma_w V_w^T = (V_w \Sigma_w^T U_w^T U_w \Sigma_w V_w^T) + \Sigma_w^2 \). Thus, this condition implies the third term in (56) is identical to:

\[
V_w \Sigma_w^T U_w^T U_w \Sigma_w V_w^T = \Sigma_w^T U_w^T U_w \Sigma_w^* V_w^T
\]

(59)

At the end, the last term in (56) can be alternatively computed as follows:

\[
V_w \Sigma_w^T U_w^T U_w \Sigma_w V_w^T = V_w \Sigma_w^T \Sigma_w V_w^T = V_w \Sigma_w^T \Sigma_w V_w^T = \Sigma_w^T \Sigma_w
\]

(60)

The SE between \( W \) and \( W^* \) can be further calculated by substituting (57) to (60) into (56) as

\[
\text{Tr} \left\{ \Sigma_w^T \Sigma_w - \Sigma_w^T U_w^T U_w^* \Sigma_w^* - \Sigma_w^T U_w^T U_w^* \Sigma_w^* + \Sigma_w^T \Sigma_w^* \right\}.
\]

(61)

With the help of unitary property of SVD computation, i.e., \( U_w^T U_w = I \), the first term in (61) can also be defined as:

\[
\Sigma_w^T \Sigma_w = \Sigma_w^T U_w^T U_w \Sigma_w
\]

(62)

In addition, another unitary property gives the result \( U_w^* U_w^* = I \). Thus, the last term in (61) can be rewritten as follows:

\[
\Sigma_w^T \Sigma_w^* = \Sigma_w^T U_w^* U_w^* \Sigma_w^*
\]

(63)

Substituting (62) and (63) into (61) yields the following result:

\[
\text{Tr} \left\{ \Sigma_w^T U_w^T U_w \Sigma_w - 2 \Sigma_w^T U_w \Sigma_w \Sigma_w^* + \Sigma_w^* U_w^T U_w \Sigma_w^* \right\}
\]

(64)
Table 3. Effect of changing principal components in terms of the SE value.

| Images          | \|A, B\|^2 | \|U_2\Sigma_2 U_2^T\|^2 |
|-----------------|-----------|-------------------------|
| 1               | 1.445E + 09 | 1.445E + 09             |
| 2               | 2.301E + 09 | 2.301E + 09             |
| 3               | 8.903E + 08 | 8.903E + 08             |
| 4               | 1.138E + 09 | 1.138E + 09             |
| 5               | 8.558E + 08 | 8.558E + 08             |
| 6               | 8.614E + 08 | 8.614E + 08             |
| Average         | 1.249E + 09 | 1.249E + 09             |

Table 4. Effect of changing principal components in terms of the PSNR score.

| Images          | PSNR(A, B) | PSNR(U_2\Sigma_2 U_2^T) |
|-----------------|------------|--------------------------|
| 1               | 10.72 dB   | 10.72 dB                 |
| 2               | 9.70 dB    | 9.70 dB                  |
| 3               | 12.82 dB   | 12.82 dB                 |
| 4               | 11.75 dB   | 11.75 dB                 |
| 5               | 12.99 dB   | 12.99 dB                 |
| 6               | 12.96 dB   | 12.96 dB                 |
| Average         | 11.66 dB   | 11.66 dB                 |

With simple algebraic manipulation, the form (65) drives the following

\[
\text{Tr} \left\{ (U_w \Sigma_w)^T U_w \Sigma_w - 2(U_w \Sigma_w)^T U_w^* \Sigma_w^* + (U_w^* \Sigma_w^*)^T U_w^* \Sigma_w^* \right\} = \text{Tr} \left\{ (U_w \Sigma_w - U_w^* \Sigma_w^*)^T (U_w \Sigma_w - U_w^* \Sigma_w^*) \right\} = \| U_w \Sigma_w - U_w^* \Sigma_w^* \|^2_2 \tag{65}
\]

From (65), it concludes the SE between \( W \) and \( W^* \) are simply Euclidean norm of difference between their principal components. Specifically, the SE is given as \( \| W - W^* \|^2_2 = \| U_w \Sigma_w V_w^T - U_w^* \Sigma_w^* V_w^T \|^2_2 = \| U_w \Sigma_w - U_w^* \Sigma_w^* \|^2_2 \). From this observation, the SE score between \( W \) and \( W^* \) is only determined by the difference between their principal components. In accordance with the PSNR value, the similarity between \( W \) and \( W^* \) can be objectively measured using the PSNR \((W, W^*) = 10 \log_{10} \frac{1}{MN} \| W - W^* \|^2 \)

Since the \( \| W - W^* \|^2_2 \) is identical to \( \| U_w \Sigma_w - U_w^* \Sigma_w^* \|^2_2 \), the PSNR score can be alternatively assessed with the metric \( 10 \log_{10} \frac{1}{MN} \| U_w \Sigma_w - U_w^* \Sigma_w^* \|^2_2 \). The difference between the principal components of \( W \) and \( W^* \) determines the PSNR value. If the difference is relatively small, it implies the PSNR value between \( W \) and \( W^* \) will be high enough, and vice versa.

We examine the effect of changing the principal components of the Lena image in Fig. 2 (a) with the principal components of the images in Fig. 9. Figure 11 shows a reconstructed Lena image set while its principal components are exchanged with the principal components of Fig. 9. One obtains nothing by exchanging the principal components over two images. This conclusion is also supported by the experimental finding, as summarized in Tables 3 and 4. The SE and PSNR between two images are simply determined with the SE and PSNR between their principal components, respectively. Thus, the choice of principal components for watermark embedding is better in comparison to the SVM. This is the main reason for the proposed method, which embeds the principal components into the host cover or host video sequences.

V. THEORETICAL ANALYSIS IN TERMS OF NORMALIZED CORRELATION COEFFICIENT

The NCC measures the similarity between the original watermark image and extracted watermark image. The different watermark insertion strategies yield different NCC values. The former scheme embeds the singular values of the watermark image into the host image. This leads to a higher NCC score. The proposed method inserts the principal components of the watermark image to produce a lower NCC score. This issue is further elaborated in the following subsection.

A. EFFECT OF EMBEDDING A SINGULAR VALUE

The former scheme embeds the SVM of watermark image into the host image. This technique induces FPP. The extracted watermark image is often with a high NCC value. The high NCC score can be explained as follows. Suppose \( W \) and \( W^* \) denote the original watermark and extracted watermark image, respectively. These two matrices own identical left and right singular vectors, but they have a different SVM. Specifically, these two matrices are denoted as \( W \leftarrow U_w \Sigma_w V_w^T \) and \( W^* \leftarrow U_w^* \Sigma_w^* V_w^T \). Beside of computation in (2), the NCC value between \( W \) and \( W^* \) can be alternatively calculated as follows:

\[
\text{NCC}(W, W^*) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) W^*(i,j)}{\sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i,j) \left[ \sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i,j) \right]} \tag{66}
\]

where \((i,j)\) denotes the spatial pixel position. Note, \( W \) and \( W^* \) in (66) are in the normalized version. As similar to SE between \( W \) and \( W^* \), the NCC between these two matrices
can also be analytic derived. With the help of matrix trace computation, the first term in (66) can be rewritten as
\[
\sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) W^*(i, j) = \text{Trace} \left\{ W^T W^* \right\}
\]
\[
= \text{Trace} \left\{ \left( W_u \Sigma_w V_w^T \right)^T U_w \Sigma_w^* V_w^T \right\}
\]
\[
= \text{Trace} \left\{ V_w \Sigma_w^* U_w^T U_w \Sigma_w^* V_w^T \right\}
\]
(67)

From SVD unitary property, we know \( U_u^T U_w = U_u U_w^T = I \) and \( V_u V_w^T = V_u^T V_w = I \). The form in (67) can be further rewritten as
\[
\text{Trace} \left\{ V_w \Sigma_w^* V_w^T \right\} = \text{Trace} \left\{ V_w \Sigma_w^* V_w^T \right\} = \text{Trace} \left\{ \Sigma_w^* V_w^T \right\} = \text{Trace} \left\{ \Sigma_w^* I \right\} = \text{Trace} \left\{ \Sigma_w^* \right\}.
\]

With the unitary property of \( V \), the second term in (66) can be simplified as
\[
\sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i, j) = \sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) W(i, j)
\]
\[
= \text{Trace} \left\{ W^T W \right\}
\]
(68)

For the second term, we conduct similar simplification as follows:
\[
\sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i, j) = \sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) W(i, j)
\]
\[
= \text{Trace} \left\{ W^T W \right\}
\]
(69)

Substituting the matrix \( W \) with the SVD decomposed matrices, we obtain the following form:
\[
= \text{Trace} \left\{ \left( U_w \Sigma_w V_w^T \right)^T U_w \Sigma_w V_w^T \right\}
\]
\[
= \text{Trace} \left\{ V_w \Sigma_w^* U_w^T U_w \Sigma_w^* V_w^T \right\}
\]
(70)

With the unitary property of \( U_w \) and \( V_w \), the form in (69) can be rewritten as follows:
\[
= \text{Trace} \left\{ V_w \Sigma_w^* I \Sigma_w V_w^T \right\}
\]
\[
= \text{Trace} \left\{ V_w \Sigma_w^* W V_w^T \right\}
\]
\[
= \text{Trace} \left\{ \Sigma_w^* W \right\}
\]
\[
= \text{Trace} \left\{ \Sigma_w^* \right\}.
\]

Based on the fact that \( U_w^T U_w = U_w U_w^T = I \) and \( V_w V_w^T = V_w^T V_w = I \), we can further rearrange as
\[
\text{Trace} \left\{ V_w \Sigma_w^* V_w^T \right\} = \text{Trace} \left\{ V_w \Sigma_w^* V_w^T \right\} = \text{Trace} \left\{ \Sigma_w^* V_w^T \right\} = \text{Trace} \left\{ \Sigma_w^* I \right\} = \text{Trace} \left\{ \Sigma_w^* \right\}.
\]

The matrix trace tells \( \text{Trace} \left\{ \Sigma_w^* \right\} = \sum_{i=1}^{N} \sum_{j=1}^{N} W^2(i, j) \).

Thus, the third terms in (66) can be further obtained as follows:
\[
\sum_{i=1}^{M} \sum_{j=1}^{N} W^*(i, j) W^*(i, j)
\]
\[
= \sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) W(i, j)
\]
\[
= \text{Trace} \left\{ W^T W \right\}
\]
(71)

By substituting (68), (70), and (71) into (66), the NCC between \( W \) and \( W^* \) can be simplified as follows:
\[
\text{NCC} (W, W^*)
\]
\[
= \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) W^*(i, j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i, j) \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} W^2(i, j)}}}
\]
\[
= \text{NCC}(W, W^*).
\]
(72)

As it can be concluded from (72), the NCC score between \( W \) and \( W^* \) is identical to that of the NCC computation between their singular value matrices if the matrices \( W \) and \( W^* \) are only differ in their SVM. The computation is applicable for \( W \) and \( W^* \), while the normalization (centered into its mean value) process is performed or not on these two matrices.

B. EFFECT OF EMBEDDING PRINCIPAL COMPONENTS

This part gives the theoretical analysis for the proposed method which embeds the principal components of watermark image into the host image. This simple strategy avoids the FFP. Embedding the principal components of watermark image induces a lower NCC score on the extracted watermark image. This phenomenon can be mathematically explained as follows. Let \( W \) and \( W^* \) be the original and extracted watermark image, respectively. They have different principal components denoting as \( W \leftarrow U_w \Sigma_w V_w^T \) and \( W^* \leftarrow U_w^* \Sigma_w^* V_w^T \). However, the matrices \( W \) and \( W^* \) have identical right singular vector. We begin the simplification for the first terms of (66). This simplification gives the following result:

For the third term of (66), we conduct the following simplification:
\[
\sum_{i=1}^{M} \sum_{j=1}^{N} W^*(i, j) W^*(i, j)
\]
\[
= \text{Trace} \left\{ W^T W^* \right\}
\]
\[
= \text{Trace} \left\{ \left( U_w \Sigma_w V_w^T \right)^T U_w \Sigma_w V_w^T \right\}
\]
\[
= \text{Trace} \left\{ V_w \Sigma_w^* U_w^T U_w \Sigma_w^* V_w^T \right\}
\]
(73)
The second term in (66) can be simplified as follows:

\[ \sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) W(i,j) = \text{Trace} \left\{ W^T W \right\} \]  

(74)

According to (70), we know \( \text{Trace} \left\{ W^T W \right\} = \text{Trace} \left\{ \Sigma_w^T \Sigma_w \right\} \). Thus, the form in (75) can be rewritten as follows:

\[ = \text{Trace} \left\{ \Sigma_w^T \Sigma_w \right\} = \text{Trace} \left\{ \Sigma_w^T \Sigma_w I \right\} \]  

(75)

Based on the unitary property of \( U_w \), i.e. \( I = U_w^T U_w \). With simple manipulation, the form in (75) can be rearranged as

\[ = \text{Trace} \left\{ \Sigma_w^T U_w^T U_w \Sigma_w \right\} = \text{Trace} \left\{ (U_w \Sigma_w)^T (U_w \Sigma_w) \right\} \].

\[ = \sum_{i=1}^{M} \sum_{j=1}^{N} (U_w \Sigma_w) (i,j) (U_w \Sigma_w) (i,j). \]  

(76)

The last quantity indicates the second term can be represented as

\[ \sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) W(i,j) = \sum_{i=1}^{M} \sum_{j=1}^{N} (U_w \Sigma_w) (i,j) (U_w \Sigma_w) (i,j). \]

At the end, the third term can be further simplified as follows:

\[ \sum_{i=1}^{M} \sum_{j=1}^{N} W^* (i,j) W^* (i,j) = \text{Trace} \left\{ W^* T W^* \right\}. \]

Substituting \( W^* \leftarrow U_w^* \Sigma_w^* V_w^T \), we obtain the

\[ \text{Trace} \left\{ \left( U_w^* \Sigma_w^* V_w^T \right)^T U_w^* \Sigma_w^* V_w^T \right\} \]

\[ = \text{Trace} \left\{ V_w \Sigma_w^T U_w^* \Sigma_w^* V_w^T \right\} \]

\[ = \text{Trace} \left\{ \Sigma_w^T U_w^* \Sigma_w^* V_w^T \right\} \]

\[ = \text{Trace} \left\{ \Sigma_w^T U_w^* \Sigma_w^* I \right\} = \text{Trace} \left\{ (U_w^* \Sigma_w^*)^T U_w^* \Sigma_w^* \right\}. \]  

(77)

The last form indicates the third term in (77) can be simply computed based on the inner product between the principal components of \( W \) and \( W^* \).

Replacing (66) with the simplified versions of (73), (76), and (77) we obtain the following result:

As it can be seen in (78), as shown at the bottom of the next page, the NCC between \( W \) and \( W^* \) is identical to that of the NCC value between \( U_w \Sigma_w \) and \( U_w^* \Sigma_w^* \). The matrices \( U_w \) and \( U_w^* \) often consist of negative values. It indicates the multiplication results on \( U_w \Sigma_w \) and \( U_w^* \Sigma_w^* \) also have negative values. Thus, the NCC computation can also be a negative value. The principal components offer a better choice for embedding the watermark information in the video watermarking system.

Tables 5 and 6, the experimental finding on NCC computation while the SVM and principal components of watermark image, respectively, are embedded into the host image. Herein, we compute the NCC values over the image sets in Fig. 11. These two tables show the NCC between the original and extracted watermark image totally depends on the SVM and principal components. In case of the embedding SVM, Table 5 shows the relationship with the NCC score \( \text{NCC}(A,B) = \text{NCC}(\Sigma_A, \Sigma_B) \). The Table 6 proves \( \text{NCC}(A,B) = \text{NCC}(U_A \Sigma_A, U_B \Sigma_B) \) if the principal component of watermark image is embedded into the host image. Embedding principal components of watermark image gives better performance compared to that of inserting SVM image as indicated with lower NCC score. Thus, the proposed method gives better performance.

VI. EXPERIMENTAL RESULTS

The performance of the proposed method is first assessed in terms of the imperceptibility test. In this experiment, the occurrence of the watermark image in the host video is simply judged by visual investigation as well as objective measurement. Two objective metrics (PSNR and NCC) are employed to measure the proposed method performance. This section also discusses the robustness and vulnerability tests for the proposed method against various malicious attacks and FPPs. The end of this section summarizes the performance comparison in choosing a single and adaptive scaling factor for the proposed method.

A. IMPERCEPTIBILITY TEST

The performance of the proposed method is measured under the watermarked video as well as the extracted watermark image. Two criterions are used to examine the proposed method performance, i.e. visual inspection and objective assessment. The proposed method satisfies the imperceptibility aspect if the presence of the watermark cannot be visually perceived by human vision. The quality of the extracted watermark image is measured over the
NCC criterion. In addition, the PSNR score indicates the imperceptibility aspect for the watermarked video.

First, the proposed method embeds the grayscale watermark image, as shown in Fig. 4 (a) in the color host video, as given in Fig. 3 (a). The proposed method selects a suitable frame from the host video using the keyframe selection strategy for watermark information embedding. It employs a single scaling factor, $\alpha = 0.1$. Figure 12 (a) shows the watermarked video with PSNR = 39.78 dB, where Fig. 12 (b) delivers the extracted watermark image before applying the Fibonacci-Lucas image descrambling. It gives the NCC = 0.0033 for this extracted watermark image. The extracted watermark image after applying the inverse of Fibonacci-Lucas image transformation with correct scrambling secret key $K_1$, as shown in Fig. 12 (c). The proposed method yields the NCC = 0.9758 for the extracted watermark image. However, one obtains nothing if an incorrect scrambling secret key $K_2$ is applied to the extracted watermark image with NCC = 0.0143. This experiment concludes the proposed method effectively achieves the imperceptibility aspect. In addition, the security of the proposed method is improved by exploiting the Fibonacci-Lucas image scrambling.

**B. ROBUSTNESS TEST**

Extensive experiments are also conducted to further examine the proposed method performance in terms of the robustness aspect. Herein, the experiments consider the watermarked video of Fig. 12 (a). Some attacks such as common image manipulations, geometric distortions, noise addition, etc., are applied to the watermarked video. The proposed method performs well if it can successfully extract the correct watermark image from the distorted watermarked video. Figure 13 depicts a set of attacked watermarked images over various distortions and manipulations. A set of attacks corrupted in Fig. 13 are identical to that of being used in Fig. 6 of Section II. C. We attempted to extract several watermark images from watermarked video given in Fig. 13.

The effectiveness of the proposed method is measured in terms of the NCC over the extracted watermark images.

Figure 14 shows a set of extracted watermark images obtained from a set of watermarked video as given in Fig. 13. The values of NCC are respectively reported as NCC = \{0.9317, 0.8377, 0.8710, 0.9189, 0.7379, 0.7936, 0.9053, 0.7301, 0.8847, 0.9156, 0.8734, 0.4167\}. Note, the scaling factor is the same as used previously, i.e. $\alpha = 0.1$. Figure 14 shows the proposed method produces a set of watermarked images with acceptable quality. Therefore, it can be concluded the proposed method meets the indicated robustness aspect with the correct and acceptable quality of extracted watermark images. This work is robust against malicious attacks.

**C. VULNERABILITY TEST**

The occurrence of the FPP is examined for the proposed method. The vulnerability test is almost identical to that of being used to examine the former scheme. This experiment considers the watermarked video, as shown in Fig. 12 (a). The counterfeit watermark images are reconstructed by multiplying the principal components extracted from the watermarked video with the counterfeit secret keys $U_w$ and $V_w$. These two secret keys are calculated from images, as shown in Fig. 4. Figure 15 displays the extracted watermark images constructed with the malicious counterfeit secret keys. As shown in this figure, the content of all extracted watermark images

\[
\text{NCC} (W, W^*) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (U_w \Sigma_w) (i,j) (U_{w}^* \Sigma_{w}^*) (i,j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} (U_w \Sigma_w) (i,j) (U_w \Sigma_w) (i,j)} \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} (U_{w}^* \Sigma_{w}^*) (i,j) (U_{w}^* \Sigma_{w}^*) (i,j)}}
\]

\[
= \text{NCC} (U_w \Sigma_w, U_{w}^* \Sigma_{w}^*)
\]

(78)
FIGURE 14. Extracted watermark images obtained from corrupted watermarked videos by the proposed SVD-based video watermarking scheme.

FIGURE 15. FPP test for the proposed SVD-based video watermarking scheme: (a),(c),(e) The extracted watermark images. (b),(d),(f) The descrambled watermark images with correct secret keys $K_1$. cannot be recognizable, even though one utilizes the correct secret key in the inverse Fibonacci-Lucas image descrambling step. The NCC for Fig. 15 (a)-(f) are respectively given as $NCC = \{5.9596 \times 10^{-04}, -0.0034, -0.0051, 0.0017, -4.1248 \times 10^{-04}, 8.5542e \times 10^{-04}\}$. It can be said the proposed method can resist the vulnerability attack test. Therefore, the FPP in the SVD-based video watermarking scheme can be easily solved by embedding the principal components of the watermark information into the host video or cover media.

D. EFFECT OF IMAGE SCRAMBLING METHOD AND ADAPTIVE SCALING FACTOR ON THE SVD-BASED VIDEO WATERMARKING SCHEME

This experiment investigates all videos, as shown in Fig. 3 for the host video or cover media. All watermark images in Fig. 4 are also considered to test the proposed method performance. Each watermark image is embedded into the each host video after applying the video keyframe selection, as mentioned in former method. The quality of the watermarked images is further calculated in terms of the PSNR by averaging its value over all watermarked images. Herein, a single scaling factor is used. We examine the scaling factor in the range $[-2,2]$. Figure 16 (a) reports the comparison in terms of average PSNR values over various scaling factors. The effect of the image scrambling method, i.e. Fibonacci-Lucas transform, is compared against the proposed method without image scrambling. Under the same scaling factor, the proposed method without image scrambling gives a better performance compared to that of the proposed method with the image scrambling. This experiment overlooks the effect of image scrambling for the extracted watermark image. In this case, a set of watermark images are extracted from several watermark videos as previously used. The quality of the extracted watermark image is examined by averaging the NCC scores over all extracted watermark images with various scaling factor. Figure 16 (b) displays the performance comparisons of the proposed method with and without the image scrambling technique in terms of average NCC values. In contrast to the previous experiment, the proposed method with image scrambling yields better NCC performance than the proposed scheme without image scrambling. The Fibonacci-Lucas image scrambling increases the robustness aspect of the proposed method.

The effects of the single and adaptive scaling factors are further examined in this experiment. The performances of the proposed method with a single and adaptive scaling factor
are examined over all videos in Fig. 3 as host videos and all images in Fig. 4 as watermark image. The comparison is conducted in terms of average scores. The performance comparison for the proposed method with a single and adaptive scaling factor over various malicious attacks, as shown in Fig. 17. The proposed method with an adaptive scaling factor is more robust against various attacks compared to that using a single scaling factor. Table 7 also supports this conclusion. Even though the proposed method with an adaptive scaling factor yields lower PSNR, it can resist various attacks on the watermarked image. Thus, this work can be regarded as a good candidate for applying the image watermarking technique in the IoT environment.

**VII. CONCLUSIONS**

A new technique on the SVD-based video watermarking scheme has been presented in this work. This technique overcomes the FPP occurring in the former existing scheme. The proposed method hides the principal components of the watermark image in the host image. This simple technique yields good performance in terms of imperceptibility aspect as well as the robustness issue. In addition, the adaptive scaling factor gives a more robust ability for the proposed method. In future work, the determination of scaling factor will be viewed as an optimization problem. The optimized scaling factor will hopefully increase the robustness and other aspects of the proposed SVD-based video watermarking scheme.

**ACKNOWLEDGMENT**

The authors would like to thank the anonymous reviewers of their articles for the many helpful suggestions.

**REFERENCES**

[1] S. Rastegar, F. Namazi, K. Yaghaeie, and A. Aliabadian, “Hybrid watermarking based on singular value decomposition and Radon transform,” *AEU-Int. J. Electron. Commun.*, vol. 65, no. 7, pp. 658–663, 2011.

[2] G. Bhattacharjee, “A new facet in robust digital watermarking framework,” *AEU-Int. J. Electron. Commun.*, vol. 66, no. 4, pp. 275–285, Apr. 2012.

[3] G. Bhattacharjee and Q. M. Jonathan Wu, “Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform,” *Future Gener. Comput. Syst.*, vol. 29, no. 1, pp. 182–195, Jan. 2013.

[4] C. Song, S. Sudirman, and M. Merabi, “A robust region-adaptive dual image watermarking technique,” *J. Vis. Commun. Image Represent.*, vol. 23, no. 3, pp. 549–568, Apr. 2012.

[5] G. Bhattacharjee, Q. M. J. Wu, and B. Raman, “A new robust logo watermarking scheme,” *Comput. Secur.*, vol. 31, no. 1, pp. 40–58, Feb. 2012.

[6] G. Bhattacharjee, B. Raman, and Q. M. J. Wu, “Robust watermarking using fractional wavelet packet transform,” *IET Image Process.*, vol. 6, no. 4, pp. 386–397, 2012.

[7] E. Yen and L.-H. Lin, “Rubik’s cube watermarking technology for grayscale images,” *Expert Syst. Appl.*, vol. 37, no. 6, pp. 4033–4039, 2010.

[8] W. El-Shafai, E.-S.-M. El-Rabaie, M. El-Halawany, and F. E. A. El-Samie, “Efficient multi-level security for robust 3D color-plus-depth HEVC,” *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30911–30937, Dec. 2018.

[9] P. Vaidya and C. Mouli, “A robust semi-blind watermarking for color images based on multiple decompositions,” *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 25623–25656, Dec. 2017.

[10] A. Zear, A. K. Singh, and P. Kumar, “A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine,” *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4863–4882, Feb. 2018.

[11] G. Bhattacharjee and Q. M. J. Wu, “A new robust and efficient multiple watermarking scheme,” *Multimedia Tools Appl.*, vol. 74, no. 19, pp. 8421–8444, Oct. 2015.

[12] P. Singh, B. Raman, and P. P. Roy, “A multimodal biometric watermarking system for digital images in redundant discrete wavelet transform,” *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3871–3897, Feb. 2017.

[13] S. Ponni and S. Ramakrishnan, “Fibonacci based key frame selection and scrambling for video watermarking in DWT-SVD domain,” *Wireless Pers. Commun.*, vol. 102, no. 2, pp. 2011–2031, Sep. 2018.

[14] S. P. Singh and G. Bhattacharjee, “A new robust watermarking system in integer DCT domain,” *J. Vis. Commun. Image Represent.*, vol. 53, pp. 86–101, May 2018.

[15] P. Singh and B. Raman, “Reversible data hiding based on Shamir’s secret sharing for color images over cloud,” *Inf. Sci.*, vol. 422, pp. 77–97, Jan. 2018.

[16] P. Singh, B. Raman, and M. Misra, “A secure image sharing scheme based on SVD and fractional Fourier transform,” *Signal Process., Image Commun.*, vol. 57, pp. 46–59, Sep. 2017.

[17] M. Mardanpour and M. A. Z. Chahooki, “Robust transparent image watermarking with shearlet transform and bidiagonal singular value decomposition,” *AEU-Int. J. Electron. Commun.*, vol. 70, no. 6, pp. 790–798, Jun. 2016.

[18] J.-M. Guo, D. Riyono, and H. Prasetyo, “Hyperchaos permutation on false-positive-free SVD-based image watermarking,” *Multimedia Tools Appl.*, vol. 78, no. 20, pp. 29229–29270, Oct. 2019.

[19] H. Prasetyo and J. M. Guo, “A note on multiple secret sharing using Chinese remainder theorem and exclusive-OR,” *IEEE Access*, vol. 7, pp. 37473–37497, 2019.

[20] J.-M. Guo, D. R. Riyono, and H. Prasetyo, “Improved beta chaotic image encryption for multiple secret sharing,” *IEEE Access*, vol. 6, pp. 46297–46321, 2018.

[21] H. Prasetyo and C.-H. Hsia, “Improved multiple secret sharing using generalized chaotic image scrambling,” *Multimedia Tools Appl.*, vol. 78, no. 20, pp. 29089–29120, Oct. 2019.

[22] M. Ali, C. W. Ahn, M. Pant, and P. Siarry, “A reliable image watermarking scheme based on redirected image normalization and SVD,” *Discrete Dyn. Nature Soc.*, vol. 2016, pp. 1–15, Feb. 2016.
HERI PRASETYO received the bachelor’s degree from the Department of Informatics Engineering, Institut Teknologi Sepuluh Nopember (ITS), Indonesia, in 2006, the master’s degree from the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taiwan, in 2009, and the Ph.D. degree from the Department of Electrical Engineering, National Taiwan University of Science and Technology, in 2015. His research interests include multimedia signal processing, computational intelligence, pattern recognition, and machine learning.

CHIH-HSIEN HSIA (Member, IEEE) was born in Taipei, Taiwan, in 1979. He received the Ph.D. degree from Tamkang University, New Taipei, Taiwan, in 2010. In 2007, he was a Visiting Scholar with Iowa State University, Ames, IA, USA. From 2010 to 2013, he was a Postdoctoral Research Fellow with the Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. From 2013 to 2015, he was an Assistant Professor with the Department of Electrical Engineering, Chinese Culture University, Taiwan. He was an Associate Professor with the Department of Electrical Engineering, Chinese Culture University, from 2015 to 2017. He is currently an Associate Professor with the Department of Computer Science and Information Engineering, National Ilan University, Taiwan. His research interests include DSP IC design, multimedia signal processing, and cognitive learning.

CHIN-HUA LIU was born in Kaohsiung City, Taiwan, in 1996. He received the B.S. degree from the Department of Electrical Engineering, Chinese Culture University, Taipei, Taiwan, in 2018. He is currently pursuing the master’s degree with the Department of Computer Science and Information Engineering, National Ilan University, Taiwan. His research interests include computer vision and image processing.