IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Secure Image-authentication Schemes with Hidden Double Random-phase Encoding

Faliu Yi[1], Youhyun Kim[2], Inkyu Moon[2], Member, IEEE

[1]Department of Clinical Science, University of Texas Southwestern Medical Center, Dallas, TX, 75390, USA
[2]Department of Robotics Engineering, DGIST, 333 Techno Jungang-daero, Hyeonpung-myeon, Dalseong-gun, Daegu, 42988 South Korea

Corresponding author: Inkyu Moon (e-mail: inkyu.moon@dgist.ac.kr).

"This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2015R1A2A1A10052566)."

ABSTRACT We present a new image-authentication algorithm based on binary-quantified double random phase encoding (DRPE) and a discrete cosine transformation (DCT)-domain watermarking scheme. The image is encrypted using a DRPE scheme, in which only the phase part of the encoded image is preserved. Then this phase image is quantified to become a binary image by giving 0 to these phase values that are less than 0 and setting others to 1. Then the quantified binary image is secretly inserted into a host image with a DCT-domain watermarking algorithm. During image authentication, the receiver gets the binary image from the watermarked image using an inverse DCT operation and codes 0 values as $-\pi$ and values of 1 as π to create a phase image. Finally, the input image is decoded from the retrieved phase image based on a double random phase decryption technique and is further authenticated using a nonlinear cross-correlation method. The present image-authentication algorithm offers an additional layer of system security because the hidden binary image reveals no information that is from the original image. Moreover, the image decrypted from the retrieved phase image cannot be easily recognized with naked eyes. However, it can be successfully authenticated by nonlinear cross-correlation, even in the face of attacks including noise attacks, filtering attacks, partial occlusion attacks, or geometric transformation attacks to the watermarked image. Our simulation results demonstrated the capability of the proposed image-authentication technique.

INDEX TERMS Information security, Three-dimensional information processing, Double random phase encoding, Discrete cosine transformation

I. INTRODUCTION

More and more attention has been paid to information security as the importance of digital information in our society, particularly in military, medical, and cloud-computing fields [1–10]. Therefore, researchers have proposed a lot of different algorithms to handle information security issues [2–4, 8–17]. Among these issues, the security of images, which are used frequently in daily life due to their ability to present information vividly and intuitively, has become increasingly important. Consequently, encryption and authentication algorithms based on images have been studied extensively [1, 7, 12, 14–22]. In the current study, we focused on image authentication based on optical encryption and information-hiding techniques. Compared to traditional block encryption algorithms [23], optical encryption techniques have a series of advantages such as multiple-dimensional and parallel characteristics. Many optics-based encryption algorithms are proposed and studied recently [13–16, 19, 20]. Information hiding as a type of steganography technique is the ability to prevent the sender and the recipient realizing that there is secret information in the sending content such as image and video [24].

Double random phase encoding (DRPE) was invented as the first optical encoding scheme by Refregier and Javidi in 1995 [25] and has been broadly researched in the fields of image security, watermarking, and authentication. DRPE can encode an input image into an encrypted image using two statistically independent random phases. As a result, the encrypted image follows a stationary white noise. That is, the encoded image will reveal no information about the input image and cannot be predicted using any part of its information. In addition, the DRPE algorithm can be implemented at high speeds because of its parallel feature [25]. Since its introduction, numerous types of DRPE algorithm have been present, based on Fresnel, fractional Fourier, or Gyrator domains [26–28]. DRPE techniques have also been successfully applied in image

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

authentication. In several previous studies [13, 14, 22, 29-31], the DRPE algorithm was combined with a technique called photon-counting for gray and color image authentication. This method can authenticate images using sparse complex information, based on a nonlinear correlation algorithm. In other studies, [16, 18, 20], only partial phase information from a DRPE image was used in image authentication; this approach has greatly reduced the required storage size. In other approaches [12, 15], the DRPE scheme is merged into a three-dimensional (3D) integral imaging algorithm for 3D image authentication. Similarly, sparse complex information resulting from two-dimensional (2D) elemental images can be utilized for final authentication [14, 20]. The successful authentication of 3D images can be achieved with a small amount of phase values in 2D elemental images encrypted by DRPE [12, 15]. Thus, all of these methods are applicable to image authentication and can enhance the DRPE algorithm, which is potentially at risk from attacks such as chosen cipher text attacks, ciphertext-only attacks, and known plaintext attacks [32–34]. However, all of these methods implicitly assume that the encrypted images are successfully received by the receiver and that there have been no any attacks during image transmission. Such systems will fail to authenticate the images, even when the encrypted images have been polluted by noise during internet transmission, which is a common occurrence in reality. In one recent study [35], the encrypted image was hidden within a host image using the least significant bit (LSB) technique, which can distract the attention of attackers to avoid some types of attack. Unfortunately, the LSB technique cannot resist very simple attacks, such as noise attacks and filtering attacks. Consequently, we propose hiding the encrypted information within the host image using a discrete cosine transformation (DCT) watermarking technique [36], which is robust to a number of attacks including noise attacks, filtering attacks, and geometric transformation attacks. This work can be viewed as the extension of our previous method present in [35] while the current algorithm can enhance the authentication system by utilizing a more robust hiding technique. Moreover, a series of attacks such as adding noise attacks, filtering attacks, and geometric transformation attacks are conducted in this study.

In our present image-authentication method, the DRPE technique is first applied to the input image that requires verification. The phase part of the encrypted image is reserved and then quantified into a binary image by giving 0 to these phase values that is less than 0 and setting all others to 1. This process produces a very sparse binary image. To facilitate data transmission and information security, the binary image is further inserted into a host image using a DCT watermarking algorithm, allowing the watermarked image to be transmitted via the internet without drawing the attention of attackers. Moreover, the binary image can be better preserved during data transmission because DCT watermarking is robust to attacks that might occur during transmission processing. The receiver uses the inverse operation of DCT watermarking to extract the binary image and then decode it into a phase image by assigning zero values to $-\pi$ and values of 1 to π. During this step, some original phase information is lost, and only a small part of the phase information remains the same. Thus, the decoded phase image can be considered a sparse phase image [16, 20]. Next, the obtained phase image is decoded using a double random phase decryption method. The decrypted image cannot be visually recognized because it is decrypted from a sparse phase image [14, 16], providing the system an additional layer of security because it can mislead attackers. Although the decoded image is not easily recognized with naked eyes, a nonlinear cross-correlation algorithm can authenticate it. Simulation results have shown that the present algorithm can successfully authenticate test images. Furthermore, image authentication can be achieved even when the watermarked images have experienced attacks such as noise attacks, filtering attacks, and geometric transformation attacks. It is also verified that the proposed authentication scheme is robust to partial occlusion attack and the analysis of key sensitivity shows that a successful authentication can be achieved when the error in the key is not bigger than 20%.

The organization of this paper is as follows. Section 2 gives the principle behind the DRPE technique. Section 3 describes the discrete cosine transformation watermarking algorithm. Section 4 sketches the image authentication procedure. Section 5 shows the experimental results. Section 6 concludes this paper.

II. THE DRPE TECHNIQUE

The DRPE technique has been widely studied as an important optical security system for images due to its parallel processing property and easy configuration [25]. Figure 1 provides a graphic diagram of a DRPE system in the Fourier domain. The input image $I(x,y)$ is first encoded into an image $E(\xi,\eta)$ that satisfies with stationary white noise using two random phase masks $m_1=\exp(j2\pi n(x,y))$ and $m_2=\exp(j2\pi b(\mu,\nu))$, where $n(x,y)$ and $b(\mu,\nu)$ are uniformly distributed between 0 and 1, exp() indicates the natural exponential function, and j is the imaginary unit. Typically, phase mask m_1 and m_2 are located in the input image plane and the Fourier domain, respectively. Then for DRPE systems in the Gyrator, fractional Fourier, or Fresnel domain, m_2 is placed in its corresponding Gyrator, fractional Fourier, or Fresnel domain [26–28]. The mathematically expression of DRPE processing in the Fourier domain can also be shown as follows [13, 25]:

$$E(\xi,\eta) = FT^{-1}[FT[I(x,y)\exp(j2\pi n(x,y))]\exp(j2\pi b(u,\nu))] \quad (1)$$

where FT and FT^{-1} represent a 2D Fourier transform and an inverse Fourier transform, respectively. Similarly, double random phase decryption, which is the reverse procedure of DRPE, can be mathematically described as following equation [13, 25].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

$$D(x,y)=\left|FT^{-1}[FT[E(\xi,\eta)]\exp(j2\pi b(u,v))]\right| \tag{2}$$

where $D(x,y)$ is the decrypted image and $|\cdot|$ indicates the modulus operation. The intensity of the decrypted image is not affected by the first phase mask m_1 in DRPE system due to the modulus operation and it is removed from the decryption equation (Eq. 2) to measure the decrypted image [25]. Several applications of the DRPE technique have been explored in previous studies [1, 14, 16, 26].

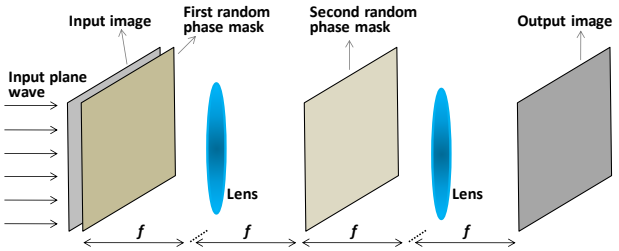


FIGURE 1. Graphic diagram of the double random phase encryption (DRPE) system in the Fourier domain.

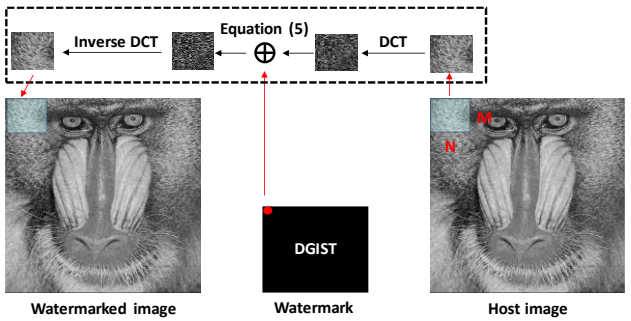


FIGURE 2. The process of block discrete cosine transformation (DCT) watermarking.

III. DCT WATERMARKING

Digital watermarking is the process of inserting data into digital multimedia content such as still audio, images, and video. This process is widely applied in copyright protection, as well as identity and banknote authentication [37]. There are two main watermarking techniques, one based on the spatial domain and the other on the frequency domain; the latter is the basis for the DCT watermarking method applied in this study. The basic approach of DCT watermarking is to insert a watermark within the frequency. In the current study, the watermark is a binary image and the host is an image whose size is $M\times N$ times of that of the watermark image and we adopted block-based DCT watermarking for hidden information [36–38]. The host image is divided into a series of $M \times N$ blocks, and a 2D DCT is applied to each block; the DCT operation is described as follows:

$$F(u,v)=\alpha_u\alpha_v\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}f(m,n)\cos\frac{\pi(2m+1)u}{2M}\cos\frac{\pi(2n+1)v}{2N} \tag{3}$$

where M and N are the rows and columns of the image block $f(m,n)$, $0\le u\le M-1, 0\le v\le N-1$, the values $F(u,v)$ are the DCT coefficients of the image block $f(m,n)$, and α_u and α_v are given as follows:

$$\alpha_u=\begin{cases}\dfrac{1}{\sqrt{M}}, & u=0\\ \sqrt{\dfrac{2}{M}}, & 1\le u\le M-1\end{cases},\quad \alpha_v=\begin{cases}\dfrac{1}{\sqrt{N}}, & v=0\\ \sqrt{\dfrac{2}{N}}, & 1\le v\le N-1\end{cases} \tag{4}$$

Then the intensity value w in watermark image I is inserted into the DCT coefficients of the corresponding host image block as follows:

$$F'(u,v)=\begin{cases}F(u,v)(1-\alpha), & w=0\\ F(u,v)(1+\alpha), & w=1\end{cases} \tag{5}$$

where $F'(u,v)$ denotes the DCT coefficients with watermark information w embedded, and α is the embedding parameter, which controls the strength of DCT coefficient modification. Finally, the modified DCT coefficient with information embedded should be transformed from the frequency domain to the spatial domain using the inverse DCT equation as follows:

$$f'(m,n)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v F'(u,v)\cos\frac{\pi(2m+1)u}{2M}\cos\frac{\pi(2n+1)v}{2N} \tag{6}$$

where $f'(m,n)$ is the host block image in the spatial domain after embedding the watermark information and $0\le u\le M-1, 0\le v\le N-1$. The watermark can be extracted through the inverse steps of the watermarking process. Figure 2 shows the process of block DCT watermarking. The watermarked image is obtained by sequentially conducting the operations shown in the black dashed box in Figure 2, using each pixel in the watermark image and its corresponding block in the host image.

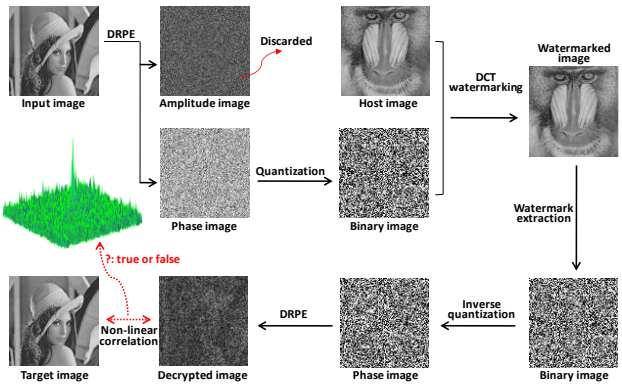


FIGURE 3. Procedure for the proposed image-authentication system.

IV. PROPOSED IMAGE-AUTHENTICATION SYSTEM

Figure 3 shows a schematic diagram of the present image-authentication system. The input image is first encrypted using the DRPE technique, in which a complex image

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

consisting of phase and amplitude information is obtained. As in previous studies [20, 39], phase information is the most import part for a successful image authentication. Therefore, we discard all of the amplitude information and retain only the phase signal in the encoded image. To better handle the phase information, we quantify it into a binary image by giving 0 to phase values <0 and 1 to the remaining values; then the binary image is hidden within a host image whose size is $M\times N$ times that of the phase image, using a DCT watermarking technique as described in section 3. We set both M and N to be 8, and α (Eq. 5) to be 0.03. Consequently, the watermarked image is freely spread through the Internet. The receiver extracts the watermark by following the inverse operation of the watermarking process. Then the binary image is transformed into a phase image by setting zero values at $-\pi$ and values of 1 at π. The converted phase image can be viewed as a sparse phase image similar to that shown in previous studies [20, 39]. This phase image is further viewed as an input image and decrypted using the double random-phase decoding technique, as present in section 2. In this step, the decrypted image is not visually recognized and can provide additional security to the system because it can easily draw the attackers' attention out of the image. In addition, an advanced statistical nonlinear cross-correlation method can be adopted to authenticate the encoded image [14–16]. The nonlinear cross-correlation transform $cc(x,y)$ between the decrypted image $d(x,y)$ and the target image $t(x,y)$ is mathematically expressed as following equation [13, 40]:

$$cc(x,y) = FT^{-1}\left\{\left|t(\mu,\eta)d(\xi,v)\right|^{k}\left[\exp(\varphi_t(\mu,\eta)-\varphi_d(\xi,v))\right]\right\} \quad (7)$$

where $t(\mu,\eta)$ and $d(\xi,v)$ are the 2D Fourier transforms of the target $t(x,y)$ and decrypted image $d(x,y)$, FT^{-1} denotes the inverse Fourier transform, and $\varphi_t(\mu,\eta)$ and $\varphi_d(\xi,v)$ are the phase signals of $t(\mu,\eta)$ and $d(\xi,v)$, respectively. The strength of the applied nonlinearity is defined by parameter k. When k=0, Eq. 7 becomes a phase extractor to enhance high-frequency signal and it is a linear filtering method when k=1. The peak-to-correlation energy (PCE) result which is defined as following equation can be used to analyze the appropriate parameter k [12].

$$PCE = \frac{\max\left[\left|cc(x,y)\right|^2\right]}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|cc(x,y)\right|^2} \quad (8)$$

where M and N are the image size along the horizonal and vertical axes; $cc(x,y)$ is the nonlinear cross correlation result between the target and the decrypted image obtained in Eq. 7; and max() is a maximum function. For the PCE value, it is the higher the better. We set the parameter k at 0.03, which is widely used in nonlinear cross-correlation evaluation [12, 22].

V. EXPERIMENTAL RESULTS

A. Image Authentication Results

We conducted numerical simulations using the Matlab R2017a software on a 64-bit Windows 10 operating system personal computer having a 16 GB of random-access memory (RAM) and 2.70 GHz Intel Core I5–7500U CPU. The true class and false class image sizes were 128×128. The size of the host image was 1024×1024. Hence, the block size parameters M and N described in section 3 were all equal to 8. Testing images, including a host, true class and false class image, are presented in Figure 4. For nonlinear cross correlation verification, the true class image shown in Figure 4 was treated as a target image.

FIGURE 4. Test images. (a) True class image, (b) false class image, and (c) host image.

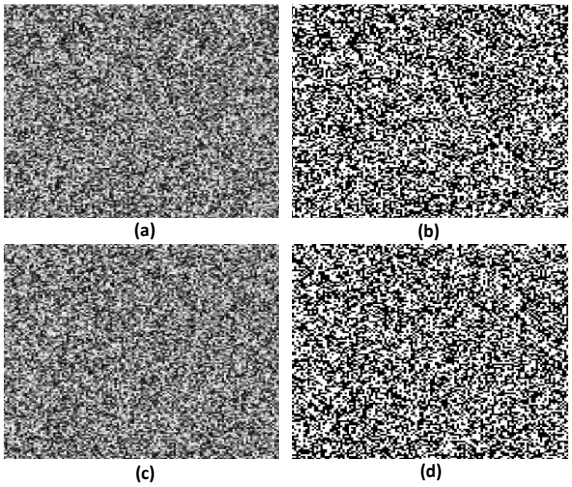


FIGURE 5. Encrypted phase and quantified binary images. (a) Encrypted phase image for the true class image; (b) quantified binary image of (a); (c) encrypted phase image for the false class image; (d) quantified binary image of (c).

As described in section 4, the input image is firstly encrypted with DRPE algorithm where the value in the encoded image is complex including both phase and amplitude information. However, we only keep the phase signal of the encoded image as shown in [20] and then quantify the phase image into a binary image by giving zero value to these locations whose phase values are less than zero and one to others. Figure 5 shows the phase image in the encrypted image and its corresponding quantified binary image for both true and false class images. After obtaining the quantified binary image, we were able to insert it into a host image with the DCT watermarking scheme described in section 3. That is, each pixel in the quantified binary image was merged into an 8 × 8 block in the host image. The watermarked image for both true and false class images are given in Figure 6.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

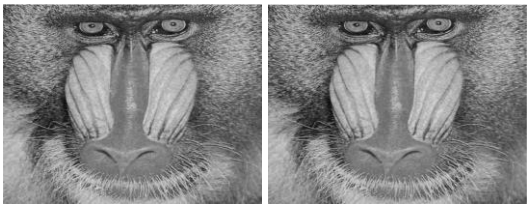


FIGURE 6. **Watermarked images. (a) Watermarked true class image and (b) watermarked false class image.**

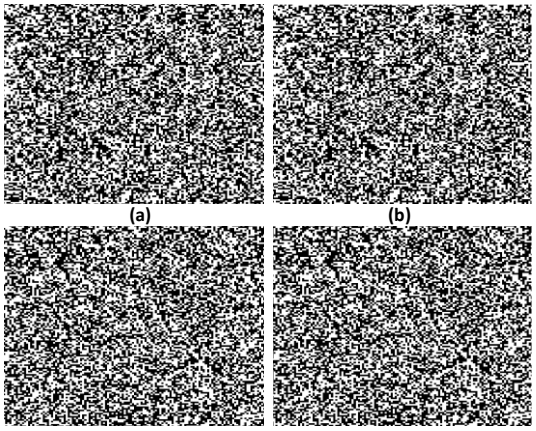


FIGURE 7. **Extracted binary and decoded phase images. (a) Extracted binary image from the true class image; (b) decoded phase image of (a); (c) extracted binary image from the false class image; (d) decoded phase image of (c).**

A comparison of the panels in Figure 6 demonstrates that the watermarked images are nearly the same as the host image shown in Figure 4c. For both the true and false class images, the peak signal-to-noise ratio (PSNR) value between the host image and the watermarked image were 44.2271 and 42.2269, respectively. Therefore, the watermarked image exhibited high quality compared to the host image itself. It was impossible to distinguish the images visually; this result is sufficient to distract potential attackers. Then the receiver extracts the watermark from the watermarked image. The watermark is a binary image created using the inverse of the DCT watermarking technique. Here, both the detector response [41] and correlation coefficient values between watermark (quantified binary image) and extracted watermark (extracted binary image) are 1.0 for both true and false class image. The phase image can be obtained from the extracted binary image by setting the zero values to $-\pi$ and all others to π. This phase image can be viewed as a spare phase image because it is not exactly the same as the phase part of the encrypted image that resulted from DRPE; however, it contains partial phase information. As studies have shown [15, 20], the partial phase image can also be successfully authenticated. The retrieved binary image and its corresponding decoded phase images are shown in Figure 7 for both true and false class images.

The decoded phase image is then fed into the double random phase decoding algorithm to create the decrypted image. Because the decoded phase image does not have all of the phase information, it is not easy to visually recognize the decrypted image, which provides another layer of security to the system, by distracting the attention of attackers. However, the encoded image which is visually unrecognizable can be verified using the nonlinear cross correlation algorithm as described in section 4. Figure 8 shows the decrypted image and authentication results for both false and true class images. The true class image can be successfully recognized due to the high peak in the center of the correlation plane between the target image and the true class image. On the other hand, there is no peak in the correlation plane between the target and the false class image. We calculated PCE values between false class and true class images with varying k values (Eq. 7); these are presented in Figure 9. These PCE values demonstrate that the true class image can be differentiated from the false class image when $k < 0.6$. Moreover, the difference in PCE values between the true and false class images reach a maximum when $k = 0.3$, the value that we chose for the nonlinear cross-correlation. We tested a total of 20 images and there were 10 images for both false and true class images, respectively. All simulation results indicated that true class images can be differentiated from false class images, verifying that this method can achieve successful image authentication.

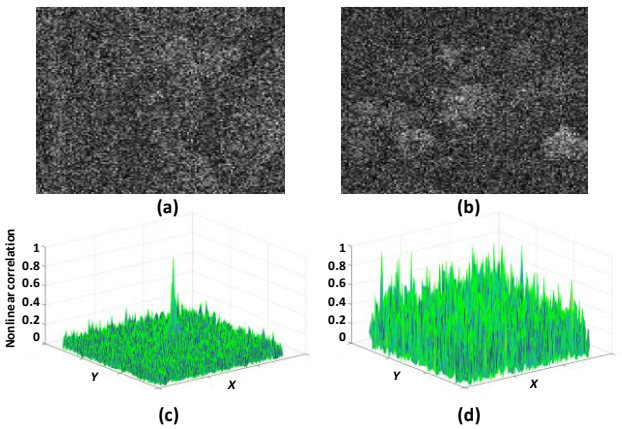


FIGURE 8. **Decrypted image and correlation planes; (a) and (c) are the decoded image and correlation plane for the true class image; (b) and (d) are the decoded image and correlation plane for the false class image.**

B. Attack Analysis

However, the watermarked image may be distorted due to noise and attacks during Internet transmission. We tested our method based on potential noise attacks, filtering attacks, and geometric transformation attacks using the true class image. Figure 10 shows a watermarked image with noise perturbance implemented by adding noise, a decrypted image from the extracted phase of a watermarked image, and the nonlinear correlation planes. To produce Gaussian noise, we set the mean to 0 and the standard deviation to 0.01. To produce salt and pepper noise, we set the noise density to 0.01. Poisson noise was generated from the watermarked image itself instead of adding noise to the watermarked

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

image. The detector response values between watermark and extracted watermark are 0.84, 0.95, and 0.98 while the correlation coefficient values are 0.68, 0.91, and 0.97 respectively for the three kinds of noise perturbance. All nonlinear cross-correlation planes exhibited high peaks at the center (Figure 10), which indicates that all images were successfully authenticated.

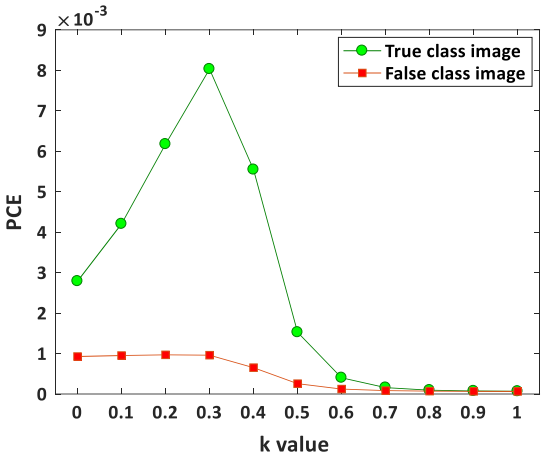


FIGURE 9. Peak-to-correlation energy (PCE) values between true class and false class images with varying *k* values

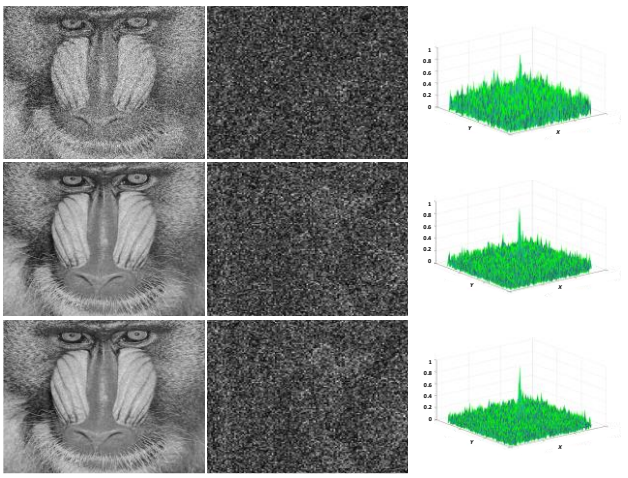


FIGURE 10. Simulated noise attacks. Rows 1–3: Gaussian noise, salt and pepper noise, and Poisson noise. Columns 1–3: watermarked images with noise, decrypted images, and nonlinear cross-correlation planes.

Figure 11 shows the results of a simulated filtering attack under the proposed algorithm. We tested the widely used median and average filtering methods [42], using a 3 × 3 neighborhood for median filtering and a 3 × 3 kernel with a value of 1/9 for average filtering. The detector response values between watermark and extracted watermark for the two filtering attacks here are 0.99 and 0.98 while the correlation coefficient values are 0.99 and 0.96. The nonlinear cross correlation plane with high peak in the center shows that the image was successfully authenticated, despite changes to the watermarked image due to the filtering method.

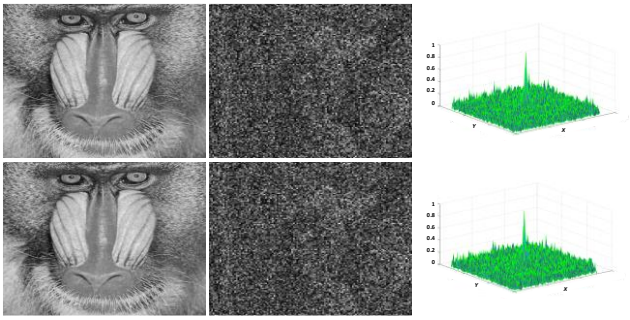


FIGURE 11. Simulated filtering attacks. Row 1: median filtering; row 2: average filtering. Columns 1–3: watermarked image after filtering, decrypted image, and nonlinear cross-correlation plane.

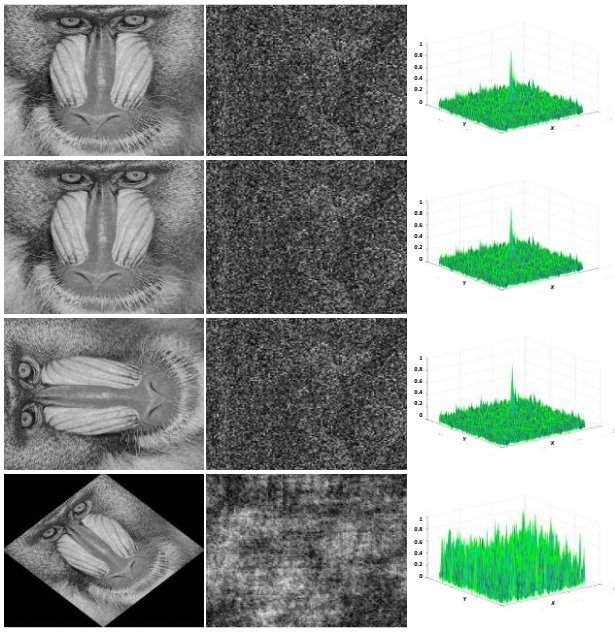


FIGURE 12. Simulated geometric transformation attacks. Rows 1–2: watermarked image scaled by ratios of 0.5 and 1.2. Rows 3–4: watermarked image rotated by 90° and 45°, respectively. Columns 1–3: watermarked images following geometric transformation, decrypted images, nonlinear cross-correlation planes.

We also simulated geometric transformation attacks on the watermarked image. The watermarked image was scaled at ratios of 0.5 and 1.2, which shrank and enlarged the image, respectively. Moreover, we rotated the watermarked image by 90° and 45°, respectively. The detector response values between watermark and extracted watermark for the two scaling and rotations are 0.99, 0.98, 0.99 and 0.23 while the correlation coefficient values are 0.99, 0.99, 0.99 and -0.001, respectively. The nonlinear cross-correlation plane results (Figure 12) illustrate that the present method was able to authenticate the image under scaling attack. However, although the method can authenticate the target image when the watermarked image was rotated by 90°, it failed when the watermarked image was rotated by 45°. Therefore, we

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

conducted further experiments; the results of these experiments demonstrate that the proposed scheme can realize image verification when the watermarked image is rotated by $(90\times n)°$, where $n \geq 0$ and an integer. However, it cannot achieve successful image authentication when the watermarked image is rotated by angles outside of this range. In such cases, too much phase signal is missed, which makes the phase image too sparse to obtain a decrypted image that can be successfully authenticated [20].

FIGURE 13. Occluded watermarked images. Left: watermarked image with 10% area occluded. Right: watermarked image with 50% area occluded.

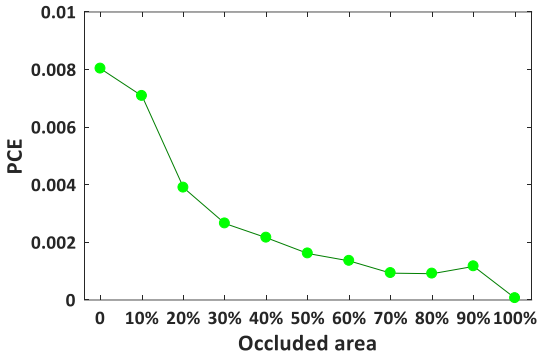


FIGURE 14. Peak-to-correlation energy (PCE) values for true class image with varied occlusion area in watermarked image.

Occlusion is another common attack in watermarked image. Here, we tested the algorithm resistance against occlusion attack by occluding the watermarked image with a percentage of area from 0% to 100% in an interval of 10%. Two of the occluded watermarked images are shown in Figure 13 where the occluded area is filled with value of zero. Consequently, the PCE values in the authentication system are shown in Figure 14 where the watermarked image is occluded with a varied percentage of area. By observing the nonlinear cross-correlation planes and comparing the PCE values in Figure 14 and those in Figure 9, we found the system can successfully authenticate the true class image when the occlusion area is less than 40% of the original watermarked image. Figure 15 shows the nonlinear cross-correlation planes for the true class image when the watermarked images are occluded with 30% and 40% of its original area. It is noted that the left image in Figure 15 has high peak at the center while the right image doesn't have.

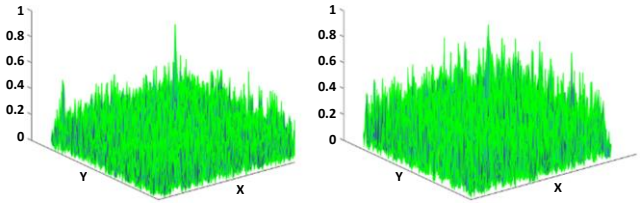


FIGURE 15. Nonlinear cross-correlation planes for true class image where 30% (Left image) and 40% (Right image) area in watermarked image are occluded.

C. Key Sensitivity Analysis

As described in Section II, the first phase key in DRPE can be discarded in the decryption process. Therefore, the key sensitivity analysis is only conducted on the second phase key. Here, we analyzed the PCE values for true class image using the key with varied number of pixel value changed. The portion of pixel number in the second phase key is changed from 0 to 100% with 10% as interval. The pixel locations with changed phase value are totally random. Figure 16 shows the PCE values that are from the corresponding key where certain portion pixel values are randomly changed. It is found from the PCE curve in Figure 16 and nonlinear cross-correlation planes in Figure 17 that the proposed algorithm cannot achieve a successful image authentication when the error in the second phase key is larger than 20%.

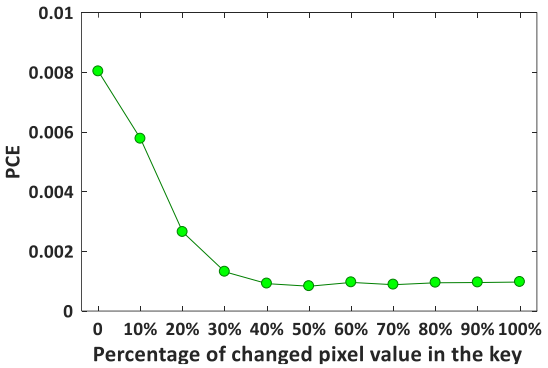


FIGURE 16. Peak-to-correlation energy (PCE) values for true class image with part of the pixel values changed in the second phase key.

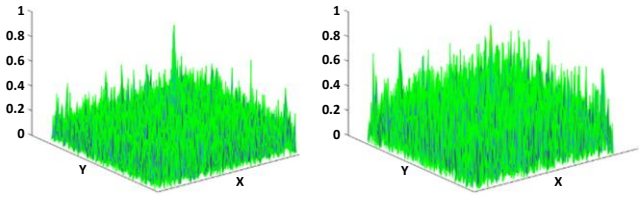


FIGURE 17. Nonlinear cross-correlation planes for true class image where 20% (Left image) and 30% (Right image) pixel in the second phase key are randomly changed.

VI. CONCLUSIONS

An image verification algorithm was proposed using DRPE and DCT-domain watermarking techniques. The phase information in an encrypted image obtained by DRPE is binary quantified and then embedded within a host image through the DCT watermarking method. The quantified

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

image reveals no information from the original image, even if it is successfully extracted by an attacker. The receiver obtains the watermarked image and extracts the quantified image through an inverse DCT watermarking method. The quantified image is further transformed into a phase image by giving $-\pi$ to these locations having zero values and assigning π to other locations. Consequently, the decrypted image is obtained using a double random-phase decoding scheme based on the phase image. The decrypted image cannot be visually recognized, which offers another layer of security to the authentication system. However, the image can be verified using a nonlinear cross-correlation method. We verified experimentally that the proposed system can successfully differentiate a true class image from false class images. In addition, we simulated a series of attack operations including noise attacks, filtering attacks, occlusion attack, and geometric transformation attacks. The experimental results showed that the present image-authentication algorithm is robust to noise and filtering attacks. However, although the algorithm can achieve successful authentication when the watermarked image is rotated by multiples of 90°, it fails when the watermarked image is rotated by angles outside of this range. Occlusion attack simulation showed that the algorithm can achieve successful image authentication when the percentage of occlusion in the watermarked image is less than 40%. In terms of key sensitivity, the proposed algorithm fails to fulfil the authentication when the error in the second phase key is larger than 20%.

REFERENCES

[1] Y. Qin, Q. Gong, and A. Wang, "Image encoding and watermarking in the double random phase encoding scheme with sparse representation strategy," Journal of Optics, 44, 1, 45-52, 2015.

[2] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Transactions on Information Forensics and Security, 12, 10, 2402-2415, 2017.

[3] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," IEEE Transactions on Dependable and Secure Computing, 2017.

[4] J. Wang, T. Li, Y. Shi, S. Lian, and J. Ye, "Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics," Multimedia Tools and Applications, 76, 22, 23721-23737, 2017.

[5] J. Wang, S. Lian, and Y. Shi, "Hybrid multiplicative multi-watermarking in DWT domain," Multidimensional Systems and Signal Processing, 28, 2, 617-636, 2017.

[6] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, 27, 2, 340-352, 2016.

[7] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security, 11, 11, 2594-2608, 2016.

[8] S. Kishk and B. Javidi, "Watermarking of three-dimensional objects by digital holography," Optics Letters, 28, 3, 167-169, 2003..

[9] W. Gordon, A. Fairhall, and A. Landman, "Threats to information security: public health implications," New England Journal of Medicine, 377, 8, 707-709, 2017.

[10] O. Matoba, T. Nomura, E. Perez-Cabre, M. Millan, and B. Javidi, "Optical Techniques for Information Security," Proceedings of the IEEE, 97, 6, 1128-1148, 2009.

[11] B. Chen, X. Qi, X. Sun, and Y. Shi, "Quaternion pseudo-Zernike moments combining both of RGB information and depth information for color image splicing detection," Journal of Visual Communication and Image Representation, 49, 283-290, 2017.

[12] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Optics Letters, 38, 17, 3198-3201, 2013.

[13] I. Moon, F. Yi, M. Han, and J. Lee, "Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms," Applied Optics, 55, 16, 4328-4335, 2016.

[14] E. Pérez-Cabré, H. Abril, M. Millán, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," Journal of Optics, 14, 9, 094001, 2012.

[15] F. Yi, Y. Jeoung, and I. Moon, "Three-dimensional image authentication scheme using sparse phase information in double random phase encoded integral imaging," Applied Optics, 56, 15, 4381-4387, 2017.

[16] J. Zheng and X. Li, "Image authentication using only partial phase information from a double-random-phase-encrypted image in the Fresnel domain," Journal of the Optical Society of Korea, 19, 3, 241-247, 2015.

[17] Z. Zhou, C. Yang, B. Chen, X. Sun, Q. Liu, and Q. Jonathan, "Effective and efficient image copy detection with resistance to arbitrary rotation," IEICE Transactions on Information and Systems, 99, 6, 1531-1540, 2016.

[18] J. Chen, Z. Zhu, C. Fu, L. Zhang, and Y. Zhang, "Information authentication using sparse representation of double random phase encoding in fractional Fourier transform domain," Optik-International Journal for Light and Electron Optics, 136, 1-7, 2017.

[19] J. Chen, Z. Zhu, C. Fu, H. Yu, and L. Zhang, "Gyrator transform based double random phase encoding with sparse representation for information authentication," Optics & Laser Technology, 70, 50-58, 2015.

[20] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," Journal of Optics, 16, 2, 025402, 2014.

[21] X. Wang, W. Chen, and X. Chen, "Optical encryption and authentication based on phase retrieval and sparsity constraints," IEEE Photonics Journal, 7, 2, 1-10, 2015.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2880730, IEEE Access

[22] F. Yi, I. Moon, and Y. Lee, "A multispectral photon-counting double random phase encoding scheme for image authentication," Sensors, 14, 5, 8877-8894, 2014.

[23] V. Pachghare, Cryptography and information security, PHI Learning Pvt. Ltd., 2015.

[24] S. Katzenbeisser and F. Petitcolas, Information hiding, Artech House, 2016.

[25] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Optics Letters, 20, 7, 767-769, 1995.

[26] Z. Liu, Q. Guo, L. Xu, M. Ahmad, and S. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," Optics Express, 18, 11, 12033-12043, 2010.

[27] G. Situ, and J. Zhang, "Double random-phase encoding in the Fresnel domain," Optics Letters, 29, 14, 1584-1586, 2004.

[28] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Optics Letters, 25, 12, 887-889, 2000.

[29] Y. Wang, A. Markman, C. Quan, and B. Javidi, "Double-random-phase encryption with photon counting for image authentication using only the amplitude of the encrypted image," JOSA A, 33, 11, 2158-2165, 2016.

[30] I. Moon, "Color image authentication scheme via multispectral photon-counting double random phase encoding," Proceedings in Three-Dimensional Imaging, Visualization, and Display, 9495, 94950X, 2015.

[31] F. Yi, "Photon-counting double-random-phase image authentication in the Fresnel domain," Proceedings in International Conference on Cloud Computing and Security, Springer, 487-497, 2016.

[32] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Optics Letters, 30, 13, 1644-1646, 2005.

[33] Y. Frauel, A. Castro, T. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Optics Express, 15, 16, 10253-10265, 2007.

[34] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," Optics Letters, 31, 22, 3261-3263, 2006.

[35] F. Yi, Y. Jeoung, R. Geng, and I. Moon, "Image authentication based on least significant bit hiding and double random phase encoding technique," Springer, 2017.

[36] Z. Xu, Z. Wang, and Q. Lu, "Research on image watermarking algorithm based on DCT," Procedia Environmental Sciences, 10, 1129-1135, 2011.

[37] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2007.

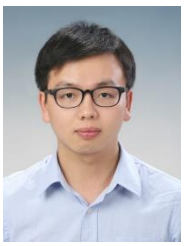
[38] V. Gupta and M. Barve, "Review on image watermarking and its techniques," International Journal of Advanced Research in Computer Science and Software Engineering," 4, 1, 92-97, 2014.

[39] W. Chen, X. Wang, and X. Chen, "Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," Journal of Optics, 17, 3, 035702, 2015.

[40] B. Javidi, "Nonlinear joint power spectrum based optical correlation," Applied Optics, 28, 12, 2358-2367, 1989.

[41] M. Noorkami, R. M. Mersereau, "Digital video watermarking in P-frames with controlled video bit-rate increase," IEEE transactions on information forensics and security, 3, 3, 441-455, 2008.

[42] R. Gonzalez, R. Woods, and S. Eddins, Digital Image Processing using MATLAB, Pearson-Prentice Hall, USA, 2004.



Faliu Yi received the BS degree in information security from Yunnan University in China in 2008. He received his ME and PhD degrees in computer engineering from Chosun University in South Korea in 2012 and 2015, respectively. He worked at the University of Texas Southwestern Medical Center as a postdoctoral researcher since 2015. He is currently a machine learning scientist at Spectral MD, Inc. His research interests include three-dimensional image processing, computer vision, machine learning, information security, and parallel computing.

Youhyun Kim received his BS and MS degrees in electronic engineering from SungKyunKwan University in South Korea in 1989 and 1997, respectively. He received his PhD degree in electrical and computer engineering from SungKyunKwan University in South Korea in 2002. He is currently a researcher at the department of robotics engineering of DGIST in South Korea. His current research interests include digital holography, optical information security, image processing, and optical information processing.

Inkyu Moon received the BS degree in electronics engineering from SungKyunKwan University in South Korea in 1996 and the PhD degree in electrical and computer engineering from the University of Connecticut, Storrs, CT, USA, in 2007. From 2009 to 2017, he was a faculty member at the department of computer engineering at Chosun University, South Korea. He joined DGIST in South Korea in 2017 and is currently an associate professor at the department of robotics engineering. He has more than 100 publications including peer-reviewed journal articles, conference proceedings and invited conference papers. His research interests include digital holography, biomedical imaging, image processing, and optical information processing. He is a member of IEEE, OSA, and SPIE.