2020

QR Code Watermarking for Digital Images

Yang-Wai Chow
University of Wollongong, caseyc@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Joon Sang Baek
University of Wollongong, baek@uow.edu.au

jongkil Kim
University of Wollongong, jongkil@uow.edu.au

QR Code Watermarking for Digital Images

Abstract

2020, Springer Nature Switzerland AG. With the growing use of online digital media, it is becoming increasingly challenging to protect copyright and intellectual property. Data hiding techniques like digital watermarking can be used to embed data within a signal for purposes such as digital rights management. This paper investigates a watermarking technique for digital images using QR codes. The advantage of using QR codes for watermarking is that properties of the QR code structure include error correction and high data capacity. This paper proposes a QR code watermarking technique, and examines its robustness and security against common digital image attacks.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Chow, Y., Susilo, W., Baek, J. & Kim, J. (2020). QR Code Watermarking for Digital Images. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11897 LNCS 25-37.

QR Code Watermarking for Digital Images

Yang-Wai Chow, Willy Susilo, Joonsang Baek, Jongkil Kim

Institute of Cybersecurity and Cryptology,
School of Computing and Information Technology,
University of Wollongong, Wollongong, Australia
{caseyc, wsusilo, baek, jongkil}@uow.edu.au

Abstract. With the growing use of online digital media, it is becoming increasingly challenging to protect copyright and intellectual property. Data hiding techniques like digital watermarking can be used to embed data within a signal for purposes such as digital rights management. This paper investigates a watermarking technique for digital images using QR codes. The advantage of using QR codes for watermarking is that properties of the QR code structure include error correction and high data capacity. This paper proposes a QR code watermarking technique, and examines its robustness and security against common digital image attacks.

Keywords: Data hiding; Discrete wavelet transform; Error correction; Images; QR code; Watermarking

1 Introduction

The extensive use, exchange and sharing of online digital media content has made the task of copyright and intellectual property protection increasingly challenging. Data hiding techniques like digital watermarking can be used for the purposes of digital rights management.

Digital watermarking is a widespread field that has been studied over many decades [4]. The idea behind watermarking is to embed additional data within a signal and be able to extract this data when required [5]. The embedding of additional data within the signal must be performed in a way that does not interfere with the normal usage of the signal. Furthermore, a successful watermark should be robust against signal alteration, up to a point at which the signal is damaged and loses its commercial value [13]. In light of this, there are four key properties that affect any watermarking system; namely, invisibility, capacity, robustness and security [4, 12].

This paper investigates a QR code watermarking technique for digital images. The purpose of this approach is to capitalize on the inherent error correction properties of the QR code structure, along with its high data capacity. The QR code error correction mechanism allows a QR code to be correctly decoded despite the presence of slight errors in the QR code, as long as the error does not exceed its error correction capacity. As such, by embedding a QR code as

a watermark within a digital image, the watermark can potentially withstand distortions to the signal, provided the QR code can be reconstructed via the watermark extraction process.

There are two primary methods for embedding watermark data within digital images in an imperceptible manner. This can be done via the spatial domain or the frequency domain. There are a number of advantages of modifying coefficients in the frequency domain, for example, it incorporates features of the human visual system more effectively, it provides the ability to spread the embedded signal in the frequency domain, and it operates in the compressed domain which is also used by most compression standards [6]. Therefore, to make the watermark imperceptible, the proposed approach uses the Discrete Wavelet Transform (DWT) technique.

The aim of the proposed QR code watermarking approach, is to embed a QR code symbol within one of the DWT sub-bands of a digital image. Within the frequency domain, the strength of the embedded watermark can be adjusted based on the desired tradeoff between imperceptibility and robustness. This paper presents the proposed technique and examines its features with respect to the key watermarking properties. In addition, the paper demonstrates the robustness and security of the proposed QR code watermarking technique against common digital image attacks, like image compression, noise, cropping, sharpening and blurring, that may be carried out by an adversary.

2 Background and Related Work

2.1 The QR Code

A QR code symbol consists of a 2D array of light and dark squares, known as modules [7]. The QR code structure contains modules for encoding data and for function patterns. Function patterns consist of finder patterns, separators, timing patterns and alignment patterns. For example, there are three identical finder patterns located at the upper left and right, and lower left corner of the symbol. The finder patterns are for a QR code reader to recognize a QR code symbol and to determine its orientation.

In addition, the QR code structure has an inherent error correction mechanism that allows data to be recovered even if a certain number of modules have been corrupted. The data capacity of a QR code depends on its version and error correction level. There are forty different QR code versions and four error correction levels; namely, L (low), M (medium), Q (quartile) and H (high), which correspond to error tolerances of approximately 7%, 15%, 25% and 30% respectively.

2.2 Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is a technique that is widely used in image and signal processing. For digital images, the DWT technique involves the

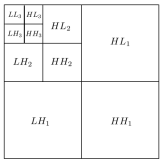


Fig. 1. DWT at level 3.

decomposition of an image into frequency channels of constant bandwidth on a logarithmic scale [9, 11].

When applying the DWT technique to a 2D image, the image is decomposed into four sub-bands, which are denoted as LL (low-low), LH (low-high), HL (high-low) and HH (high-high). Each sub-band in turn can be further decomposed at the next level, and this process can continue until the desired number of levels is achieved. In view of the fact that the human visual system is more sensitive to the LL sub-band (i.e. the low frequency component), to maintain image quality watermark information is typically embedded within one or more of the other three sub-bands [9]. Fig. 1 gives a depiction how the DWT can decompose an image into sub-bands at 3 levels. For experiments in this paper, the watermark was embedded within the HH_3 sub-band.

2.3 Arnold Transform

The Arnold transform is a invertible transform that can be used for scrambling the pixels in a digital image. The transform scrambles the pixels within an image to disrupt the correlation between adjacent pixels. As such, the Arnold transform is commonly used as part of many watermarking schemes, as it distributes the pixels over the entire image [8]. The reason for doing this is so that any error introduced by distorting a watermarked image will be scattered over the image, and the watermark can still potentially be recovered despite the error.

2.4 Related Work

There have been a variety of different uses of QR codes in the area of computer security. In previous work, Chow et al. [3] proposed the use of QR codes for watermarking using two techniques in the frequency domain. Their proposed approach combined the use of the DWT with the Discrete Cosine Transform (DCT) for QR code watermarking. In other work on QR code watermarking, an authentication method for medical images using a QR code based zero watermarking scheme was proposed [14]. In the scheme, a patient's identification details and a link their data was encoded in the form of a QR code which served as the watermark.

Kang et al. [8] proposed a watermarking approach based on the combination of DCT, QR codes and chaotic theory. In their approach, a QR code image is encrypted with a chaotic system to enhance the security of the watermark, and

embedded within DCT blocks after undergoing block based scrambling. In related work, a digital rights management method for protecting documents by repeatedly inserting a QR code into the DWT sub-band of a document was investigated [1]. Others have also proposed different QR code watermarking approaches, for example, by incorporating an attack detection feature to detect malicious interference by an attacker [15], or by embedding QR code watermarks using a just noticeable difference model to increase imperceptibility [10].

In related work on QR codes for security, Tkachenko et al. [16] described a modified QR code that could contain two storage levels. They called this a two-level QR code, as it had a public and a private storage level. The purpose of the two-level QR code was for document authentication. In addition, QR codes have also been used for secret sharing [2]. In this work, a method of distributing shares by embedding them into cover QR codes was proposed. These QR codes contained both public and private information, which allowed for the shares to be transmitted over public channels. The public information in the QR codes could be access by anyone, whereas only authorized individuals would be able to obtain the private information.

3 QR Code Watermarking

The aim of the QR code watermarking technique proposed in this paper is to embed a QR code watermark within a cover image, and to be able to extract the watermark. Fig. 2 depicts the processes involved in the embedding and extraction processes. Details of the processes will be described in the respective subsections to follow.

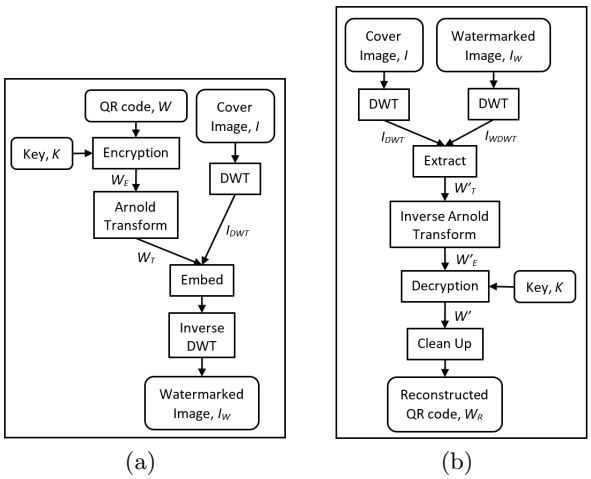


Fig. 2. Overview of the QR code watermarking processes; (a) embedding process; (b) extraction process.

3.1 Embedding Process

An overview of the embedding process is shown in Fig. 2(a). It can be seen from the figure that the embedding process accepts three inputs; a QR code, W, which is the watermark image; a key, K, for encryption; and a cover image, I. The output of the embedding process is a watermarked image, I_W.

It should be noted that K is a random bit string, which is used to encrypt and decrypt the watermark. The purpose of doing this is to ensure that even if an adversary can extract W, the adversary will not be able to obtain information about the contents of the watermark. The bits in K are to be XORed with the light and dark modules of W. As such, the length of the bit string must match the number of modules in W.

For the experiments in this paper, I was converted to DWT level 3 and the encrypted and scrambled watermark, W_T, was embedded within the HH_3 sub-band. The purpose of embedding information within the HH sub-band is due to the fact the human visual system is less sensitive to perturbations in this sub-band. The DWT coefficients C were modified based on Eq. 1 for the x and y pixels in W_T, where $W_{T,(x,y)} \in \pm 1$. The λ parameter can be adjusted to balance between watermark imperceptibility and robustness.

$$C'_{(x,y)} = C_{(x,y)} + \lambda W_{T,(x,y)}|C_{(x,y)}| \tag{1}$$

Prior to embedding the watermark, bits in the encrypted watermark were scrambled using Arnold transform. The reason for this is to distribute the watermark data over the entire image. In practice, this effectively reduces localized errors in the extracted watermark, which may result from distortions to I_W by an adversary. Algorithm 1 provides details of the steps involved in the embedding process.

Algorithm 1 Embedding algorithm

Input: A QR code, W, a cover image, I, and a key, K.
Output: A watermarked image, I_W

Step 1. Encrypt information in W by XORing the random bits in K with the modules in W to produce W_E.
Step 2. Generate a chaotic image W_T by scrambling the bits of the encrypted watermark W_E using Arnold transform over a number of iterations.
Step 3. Convert I to I_{DWT} by performing DWT to the desired level.
Step 4. Embed W_T in a I_{DWT} sub-band.
Step 5. Generate the watermarked image I_W by inversing DWT.

3.2 Extraction Process

Fig. 2(b) provides an overview of the extraction process, which is very much the reverse of the embedding process. To extract the watermark image, the extrac-

tion algorithm requires the original cover image, I; the watermarked image, I_W; and the key, K, for decryption. The output of the algorithm is the reconstructed watermark, i.e. a reconstructed QR code, W_R.

Algorithm 2 Extraction algorithm

Input: The original cover image, I, the watermarked image, I_W, and and the key, K.
Output: A reconstructed QR code, W_R

Step 1. Convert I to I_{DWT}, and I_W to I_{WDWT}, by performing DWT on the cover image and watermarked image respectively.
Step 2. Extract W'_T from differences in the specific sub-band (HH_3 in the experiments) of I_{DWT} and I_{WDWT}.
Step 3. Generate W'_E by inversing the Arnold transform.
Step 4. Decrypt W'_E using K to produce the extracted watermark image W'.
Step 5. Clean-up the W' and restore the QR code function patterns to produce W_R.

It should be noted that if I_W was distorted from attacks by an adversary, W' will result in a noisy image. Hence, a clean-up stage is required to restore the QR code. This is possible as long as information about the QR code is known; namely, the QR code version, error correction level, masking pattern and number of pixels per module. With this information, restoring the modules involves counting the total number of black and white bits for every module in W'. If there are more white bits, set the module color to white, and vice versa. Also, to ensure that the QR code is decodable, restore the QR code function patterns which may have been corrupted to produce the reconstructed QR code, W_R.

Any QR code reader should be able to decode W_R, as long as the error in W_R is below the error correction threshold of the QR code. Note that it is possible to only embed the data modules of W in I_W, since the function patterns are restored during the clean-up stage. However, in our experiments, we chose to embed the entire QR code because it provides information on the amount of noise in W', which results from distortions made to I_W. The steps involved in the extraction algorithm are provided in Algorithm 2.

4 Results and Discussion

This section presents results of experiments conducted to evaluate the proposed QR code watermarking technique. The experiments were performed using the OpenCV library on three well-known test images; namely, the Lena, Peppers and Mandrill images. These images can be seen in the tables of results shown in Tables 1, 2, and 3 respectively.

The images were all 512×512 in dimension. A QR code version 1 with error correction level H was used in the experiments. This QR code version is made

up of 21 × 21 modules. Since the HH_3 sub-band of a 512 × 512 image has a 64 × 64 resolution, we converted each module in the QR code to consist of 3 × 3 pixels, resulting in a total QR code size of 63 × 63 pixels.

4.1 Imperceptibility and Capacity

Imperceptibility is the property whereby a human cannot perceive the difference between the original and watermarked signal. The Peak Signal-to-Noise Ratio (PSNR) metric was used as a measure of image quality and to indicate the perceptibility of distortions resulting from embedding a watermark within a cover image. Fig. 3 shows a plot of the PSNR values for the test images that were obtained by varying the value of λ. Greater PSNR values indicate less difference between I and I_W. At low λ values, the human visual system is less sensitive to distortions cause by embedding the watermark. However, increasing the value of λ increases the distortion in the resulting image. When the distortion is clearly visible in I_W, the image looses its commercial value and usefulness.

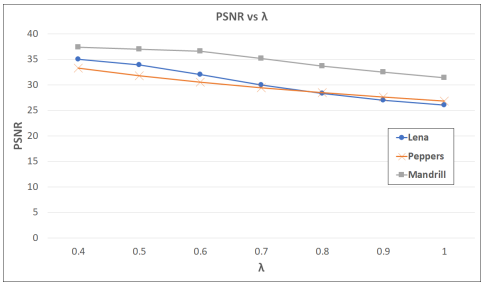


Fig. 3. PSNR values.

Capacity, or payload, is the amount of data that can be embedded by a watermarking scheme. The data capacity of the proposed watermarking technique is based on the capacity of the QR code version and error correction level of W. For a given QR code version, the higher the error correction level, the lower the data capacity, but the more robust the resulting watermark will be to errors. Hence, there is a tradeoff between data capcity and watermark robustness.

In addition, the size of W, is also governed by the size of I, since the watermark is to be embedded within a DWT sub-band of I. The higher the number of module in W, the more data the QR code can encode. However, this also means that for the watermark to be able to fit within a DWT sub-band, less pixels may have to be used to encode each module. The lower the number of pixels per module, the less robustness the watermark, because there is a higher potential for the pixels per module to the corrupted.

4.2 Robustness and Security

Robustness and security refer to a watermarking scheme's ability to withstand distortions to the watermarked signal. In the case of security, these distortions are intentional attacks by an adversary to impair the watermark [4, 12]. The robustness and security of the proposed technique was examined by applying various attacks to the watermarked images; namely, JPEG compression, sharpening, blurring, salt-and-pepper noise, and cropping. These are common attacks that are typically used to evaluate watermarking techniques.

For the JPEG compression attack, the images was compressed to 50% quality using the OpenCV library. For the sharpening and blurring attacks, basic 3×3 convolution filters were used. The weights in sharpening filter were $\begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix}$ and for blurring, a median filter $\begin{bmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \end{bmatrix}$ was used. For the salt-and-pepper noise attack, 1% of the pixels in the images were randomly overwritten with black or white pixels. Two cropping attacks were used, in the first, the image center was removed, while in the second attack, the corners of the image were removed. In both cropping attacks, a total of 25% of the images was removed.

To evaluate the amount of error in the extracted watermark and the reconstructed QR code, the Bit Error Rate (BER) and Module Error Rate (MER) metrics were used. The BER refers to the percentage of bits that were in error in the extracted watermark, W', whereas the MER is the percentage of incorrect QR code modules in the reconstructed QR code, W_R.

Tables 1, 2, and 3 demonstrate results of the various attacks on the respective test images. The results shown the tables, were obtained using $\lambda = 0.6$. For each test image and attack, the tables show the extracted watermark image and the BER, as well as the reconstructed QR code and the MER. As decribed in Section 3.2, the reconstructed QR code, W_R, was obtained after cleaning up the noise in W'. In addition, grey modules in the reconstructed QR code depict the modules that were incorrectly recovered. It should be noted that the error contained in all the reconstructed QR codes were within the error correction capacity, and thus, the recontructed QR codes could correctly be decoded.

5 Conclusion

This paper presents a QR code watermarking technique for digital images. The objective of the proposed watermarking technique is to embed a QR code within a cover image in an imperceptible manner. This was achieved by embedding a QR code within one the cover image's DWT sub-bands. The reason for using a QR code as a watermark is because the QR code structure incorporates an error correction mechanism that allows it to be correctly decoded even if it contains some error. In this paper, we discussed the properties of the proposed watermarking technique and demonstrated its robustness against common attacks that may be conducted by an adversary.

Table 1. Results on Lena.

Attack	**Attacked Image**	**Extracted Watermark, W'**	**BER**	**Reconstructed QR Code, W_R**	**MER**
Compression			21.10%		5.77%
Sharpening			16.61%		2.40%
Blurring			20.62%		4.33%
Noise			19.07%		3.85%
Cropping 1			17.74%		0.96%
Cropping 2			16.03%		1.44%

Table 2. Results on Peppers.

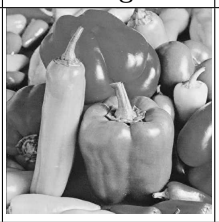
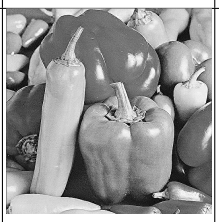
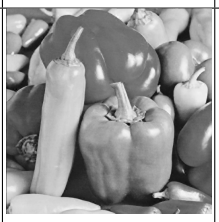
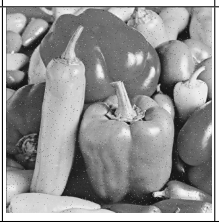
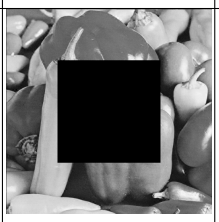
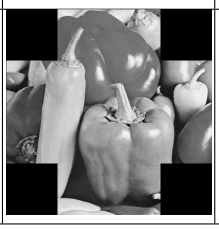
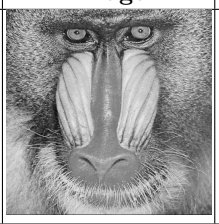
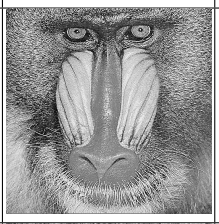
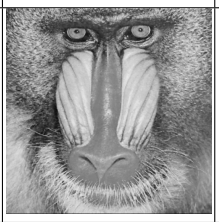
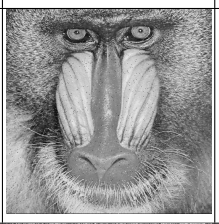
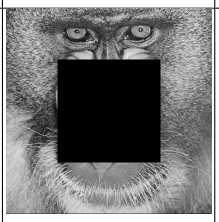
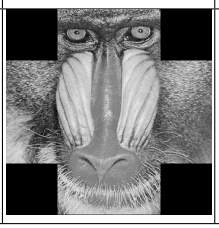
Attack	**Attacked Image**	**Extracted Watermark, W'**	**BER**	**Reconstructed QR Code, W_R**	**MER**
Compression			22.0%		4.81%
Sharpening			17.79%		5.29%
Blurring			24.04%		8.65%
Noise			19.18%		3.85%
Cropping 1			15.38%		1.44%
Cropping 2			15.92%		0.0%

Table 3. Results on Mandrill.

Attack	**Attacked Image**	**Extracted Watermark, W'**	**BER**	**Reconstructed QR Code, W_R**	**MER**
Compression			9.24%		0.0%
Sharpening			18.48%		3.85%
Blurring			21.31%		3.85%
Noise			12.44%		0.96%
Cropping 1			13.78%		0.0%
Cropping 2			14.0%		0.48%

References

1. N. Cardamone and F. d'Amore. DWT and QR code based watermarking for document DRM. In C. D. Yoo, Y. Q. Shi, H. Kim, A. Piva, and G. Kim, editors, *Digital Forensics and Watermarking - 17th International Workshop, IWDW 2018, Jeju Island, Korea, October 22-24, 2018, Proceedings*, volume 11378 of *Lecture Notes in Computer Science*, pages 137–150. Springer, 2018.
2. Y. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, and G. Yang. Cooperative secret sharing using QR codes and symmetric keys. *Symmetry*, 10(4):95, 2018.
3. Y. Chow, W. Susilo, J. Tonien, and W. Zong. A QR code watermarking approach based on the DWT-DCT technique. In J. Pieprzyk and S. Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, volume 10343 of *Lecture Notes in Computer Science*, pages 314–331. Springer, 2017.
4. I. J. Cox and M. L. Miller. The first 50 years of electronic watermarking. *EURASIP Journal on Advances in Signal Processing*, 2002(2):820936, 2002.
5. F. Hartung and M. Kutter. Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7):1079–1107, Jul 1999.
6. J. Huang, Y. Q. Shi, and Y. Shi. Embedding image watermarks in dc components. *IEEE Transactions on Circuits and Systems for Video Technology*, 10(6):974–979, Sep 2000.
7. International Organization for Standardization. Information technology — automatic identification and data capture techniques — qr code 2005 bar code symbology specification. ISO/IEC 18004:2006, 2006.
8. Q. Kang, K. Li, and J. Yang. A digital watermarking approach based on dct domain combining qr code and chaotic theory. In *2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, pages 1–7, Sept 2014.
9. C. C. Lai and C. C. Tsai. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, 59(11):3060–3063, Nov 2010.
10. H.-C. Lee, C.-R. Dong, and T.-M. Lin. Digital watermarking based on jnd model and qr code features. In *Advances in Intelligent Systems and Applications-Volume 2*, pages 141–148. Springer, 2013.
11. S. Mallat. A theory for multiresolution signal decomposition: The wavelet representation. *IEEE Trans. Pattern Anal. Mach. Intell.*, 11(7):674–693, 1989.
12. A. S. Panah, R. V. Schyndel, T. Sellis, and E. Bertino. On the properties of non-media digital watermarking: A review of state of the art techniques. *IEEE Access*, 4:2670–2704, 2016.
13. C. I. Podilchuk and E. J. Delp. Digital watermarking: algorithms and applications. *IEEE Signal Processing Magazine*, 18(4):33–46, Jul 2001.
14. V. Seenivasagam and R. Velumani. A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud. *Computational and Mathematical Methods in Medicine*, 2013(516465):16, 2013.
15. P. P. Thulasidharan and M. S. Nair. {QR} code based blind digital image watermarking with attack detection code. {*AEU*} - *International Journal of Electronics and Communications*, 69(7):1074 – 1084, 2015.
16. I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J. Gaudin, and C. Guichard. Two-level QR code for private message sharing and document authentication. *IEEE Trans. Information Forensics and Security*, 11(3):571–583, 2016.