Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 791814, 9 pages
http://dx.doi.org/10.1155/2013/791814

Research Article

Perceptual Hashing-Based Robust Image Authentication Scheme for Wireless Multimedia Sensor Networks

Hongxia Wang and Bangxu Yin

School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China

Correspondence should be addressed to Hongxia Wang; hxwang@home.swjtu.edu.cn

Received 29 January 2013; Accepted 13 March 2013

Academic Editor: Muhammad Khurram Khan

Image authentication is critical for secure image transmission and storage in a wireless multimedia sensor network (WMSN). In this paper, we propose a perceptual hashing-based robust image authentication scheme, which applies the distributed processing strategy for perceptual image hashes and can provide compactness, visual fragility, perceptual robustness, and security in digital image authentication for WMSN. In the proposed scheme, first, the cluster head node generates a secure pseudorandom chaotic sequence with keys and sends it to the image capturing node, then the image capturing node uses the received chaotic sequence to divide randomly the captured image into several overlapping rectangles, after that, two gravity centers of each rectangular region block are calculated, and finally the binary distance of the two gravity centers will be calculated in each general cluster member node. The cluster head node receives the binary sequence of the distance from all of the general cluster member nodes and combines them to form the perceptual hashing sequence to be sent to the base station for image authentication purpose. Experimental results show that the proposed scheme has satisfactory authentication ability and can ensure not only the visual fragility for perceptually distinct images but also robustness for perceptually identical images via image rotation, JPEG compression, and noise burring.

1. Introduction

Wireless sensor networks (WSNs) are going to be widely used in the near future due to their breadth of applications by military, exploration teams, researchers, and so on. Most of this research is concerned with scalar sensor networks that measure physical phenomena, such as temperature, light, humidity, pressure, acoustic sensor, or location of objects that can be conveyed through low-bandwidth and delay-tolerant data streams. Recently, the focus is shifting toward research aimed at revisiting the sensor network paradigm to enable delivery of multimedia information, such as a monitoring data, digital image, audio and video streams, as well as scalar data [1]. This effort will result in distributed, networked systems, referred to in this paper as wireless multimedia sensor networks (WMSNs). The WMSNs will enable new applications such as multimedia surveillance, traffic enforcement and control systems, advanced health care delivery, structural health monitoring, and industrial process control. Consequently, it will bring new security of challenges as well as new opportunities. Secure and robust multimedia communications become increasingly important for energy-constrained WMSNs [2]. As one of the security techniques, image authentication is critical for secure image transmission and storage in WMSNs. However, conventional data authentication schemes cannot be applied directly to WMSN due to the constraints on limited energy and computing resources in sensor nodes. Those constraints pose great challenges to WMSN development and motivate us to design a proper authentication strategy for WMSNs.

For open communication channel, WSNs are vulnerable to various attacks, and the security in WSNs is required. A secure hierarchical key management scheme in WSNs was proposed in [3]. The security analysis and simulation show the scheme can prevent several attacks effectively and reduce the energy consumption. In WSNs communications, Han et al. [4] described six types of attacks including communication attacks, attacks against privacy, sensor node targeted attacks, power consumption attacks, policy attacks, and cryptology attacks on key management. In communication attacks, eavesdropper can easily access or even manipulate message such as injecting, cropping, and tampering. So the receiver

needs to make sure that the data used in any decision-making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the networks and legitimate nodes should be able to detect messages from authorized nodes and reject them. In [5], a robust user authentication scheme for WSNs was proposed. The scheme takes an advantage of the two-factor authentication concept to provide a secure authentication system offering balanced features in terms of security and performance.

The authenticity of data and commands is also a critical requirement for the correct behavior of a WMSN [6]. Digital images are becoming widely used in WMSNs as a kind of common multimedia information. Therefore, the key establishment technique should guarantee that the image communication and storage have a way for verifying the authenticity, creditability, and integrity of the received image in WMSNs. However, resource constraints in sensor networks (such as limited battery power and bandwidth/computation capability) pose challenges for the image authentication technique. Conventional binary data authentication schemes could provide data integrity in a strict sense regardless of multimedia content. However, those schemes are not applicable to WMSNs because only simple bit errors during data transmission can lead to the authentication failing in spite of preserving multimedia content [7, 8]. On the other hand, watermarking-based image content authentication techniques are robust against bit errors, packet losses, and compression distortion. However, watermark embedding creates extra source coding overheads and complicates transmission protocol design in WMSNs [9], which don't adapt well to WMSNs due to the constraints on limited energy and computing resources.

In [10], an optimized content-aware authentication scheme for JPEG 2000 images over lossy channels was proposed. An acyclic authentication graph was developed to optimize the trade-off between the expected image distortion and the cryptohash tagging cost, through the computation based on packet loss probability and visual importance level of the image packets. The work reported in [11] proposed a JPEG 2000 compatible stream authentication scheme that significantly reduced the computational complexity and had only a minimal authentication dependency overhead in WMSNs. Moreover, an authentication-aware wireless network resource allocation scheme was developed to reduce image distortion and energy consumption during transmission. The scheme significantly improved the authenticated image quality even under strict communication energy consumption constraints in WMSN. In [12], a rate-distortion optimization authentication scheme for H.264 video transmissions was proposed. A video packet transmission scheduler was designed to minimize the visual distortion under the limitation of total bit budget and authentication dependency. Another related work regarding bite rrors robust image or video authentication was given in [13–15]. However, all of these approaches are not able to be applied directly to WMSNs due to the energy constraint. In this paper, we propose a perceptual hashing-based robust authentication scheme for WMSNs. Based on the distributed processing strategy for perceptual image hashes, the proposed scheme can provide compactness, visual fragility, perceptual robustness, and security for image authentication in WMSNs.

2. Perceptual Image Hashing Extraction

A perceptual image hashing function maps an image to a short binary string as a digest based on an image's appearance to the human eye. Perceptual image hashing is a class of one-way mappings from image presentations to a perceptual hash value in terms of their perceptual content. Given an image I and its perceptually similar copy with minor distortion I_d, the image hashing function $H_k(\cdot)$ depends on the secret key k. In [16], the desirable properties of perceptual hashing function $H_k(\cdot)$ can be summarized as follows.

(i) *One-Way Function*. Ideally, the hash generation should be noninvertible:

$$I \longmapsto H_k(I). \tag{1}$$

(ii) *Compactness*. The size of the perceptual hashing value should be much smaller than that of the original image I

$$\text{Size}\left(H_k(I)\right) \ll \text{Size}(I). \tag{2}$$

(iii) *Perceptual Robustness*. Perceptually identical images should have similar perceptual hashing values

$$\Pr\left\{H_k(I) \approx H_k\left(I_d\right)\right\} \geq 1-\varepsilon, \quad 0 \leq \varepsilon < 1. \tag{3}$$

(iv) *Visual Fragility*. Perceptually distinct images should have different perceptual hashing values

$$\Pr\left\{H_k(I) \neq H_k\left(I'\right)\right\} \geq 1-\tau, \quad 0 \leq \tau < 1. \tag{4}$$

(v) *Security*. The perceptual hashing is intractable without the secret key

$$\Pr\left\{H_k(I) \neq H_{k'}(I)\right\} \geq 1-\delta, \quad 0 \leq \delta < 1. \tag{5}$$

All of the above parameters ε, τ, and δ should be close to zero.

Based on THE above properties, perceptual image hashing can be usually applied to image content identification, image indexing, content authentication, and so forth. In particular, a perceptual hash function should have a property, that is, two images that look the same map to the same hash value, even if the images have small bit-level differences. This differentiates a perceptual hash from traditional cryptographic hashes, such as SHA-l and MD5. In cryptography, the hash function is typically used for digital signature to authenticate the message being sent so that the receiver can verify its source. A key feature of conventional hashing algorithms such as SHA-l and MD5 is that they are extremely sensitive to the input data; that is, changing even one bit of the input message will change the output dramatically. However, image data often undergoes various content-preserving manipulations such as lossy compression, channel additive

noise, image enhancement, scaling, bit errors and packet losses during wireless transmission and storage in WMSNs. These distortions are usually insignificant, and image hashes should be robust to unmalicious distortions. On the contrary, some malicious manipulations could introduce perceptually significant distortions, for example, object insertion, removal, and substitution, and it is desirable that the image hash is sensitive to perceptually significant attacks. Therefore, image hashes should be robust to unmalicious distortions, but sensitive to malicious manipulations for the image authentication purpose [17].

2.1. Image Random Blocking by Chaotic Sequence. In order to enhance the security of the perceptual hashing algorithm, we use a secure pseudorandom sequence with the key to divide randomly the digital image into C overlapping rectangles, and the key controls the number of rectangles and the pseudorandom sequence. The image blocking can also make up the disadvantage that the extracted image features can only describe global characteristics of an image.

As a phenomenon found in a nonlinear dynamic system, chaos is deterministic and random-like. Based upon the sensitive dependence of chaotic systems on their initial conditions, a large number of nonperiodic, continuous broadband frequency spectrum, noise-like, yet deterministic, and reproducible signals can be generated. So chaos is very useful for generating secure pseudorandom sequences.

The chaotic maps (6) and (7) are given by

$$Z_{n+1} = uZ_n\left(1 - Z_n\right), \quad n = 1, 2, \ldots, \tag{6}$$

$$S_{n+1} = \left(1 + 0.3\left(S_{n-1} - 1.08\right) + 379S_n^2 + 1001 \times Z_n^2\right) \bmod 3, \tag{7}$$

where $3.57 < u \leq 4$ is the chaotic system parameter and $0 < Z_1 < 1$ and $-1.5 < S_0$, $S_1 < 1.5$ are the initial values of the two chaotic systems. Z_n in formula (7) is generated by (6). When $u = 3.9$, we compute the value space of Z_1 as follows:

Suppose $Z_1 = \{0 < Z_1(i) < 1 \mid i = 1, 2, \ldots, L_1\}$ and L_1 is an integer which is large enough and generates chaotic sequences $Z = \{Z(i, j) \mid i = 1, 2, \ldots, L_1, j = 1, 2, \ldots, L_2\}$, where L_1 represents the number of chaotic sequences and L_2 means the length of each chaotic sequence. When $Z_1' = \{0 < Z_1(i) + d < 1 \mid i = 1, 2, \ldots, L_1\}$ and d is close to zero, another group of chaotic sequence $Z' = \{Z'(i, j) \mid i = 1, 2, \ldots, L_1, j = 1, 2, \ldots, L_2\}$ is generated. We use function $y = \Omega(d)$ to test the value space of Z_1 as follows:

$$y = \Omega(d) = \frac{\left[\sum_{i=1}^{L_1}\sum_{j=1}^{L_2}\left|Z(i, j) - Z'(i, j)\right|\right]}{\left(L_1 \times L_2\right)}. \tag{8}$$

The curve of function $y = \Omega(d)$ is shown in Figure 1. From Figure 1, it is seen that, when $d = 10^{-19}$, $y \approx 0$. So the value space of Z_1 is 10^{19}. Similarly, the value spaces of u, S_0, and S_1 are shown in Figures 1 and 2. They are 1×10^{15}, 3×10^{14}, and 3×10^{16}, respectively.

Therefore, when the difference of initial values or chaotic parameters of chaotic system is greater than some specific value, two different chaotic sequences will be generated. For Z_1, the difference should be greater than 10^{19} and similarly for others. Let u in (6) and S_0 as secret keys be denoted by k_1 and k_2, respectively. Consequently, we will use the generated chaotic sequences with keys k_1 and k_2 to divide randomly the digital image into C overlapping rectangles for security purpose.

According to the image size, we adaptively select proper bits of the chaotic sequence as the coordinate of x-axis and y-axis, length and width of the random region to prevent out boundary, denoted by a quaternion C (C_x, C_y, *length*, *width*). So the image is divided into C overlapping rectangular regions shown in Figure 3. Because the quaternion is randomly generated, the rectangular areas are random.

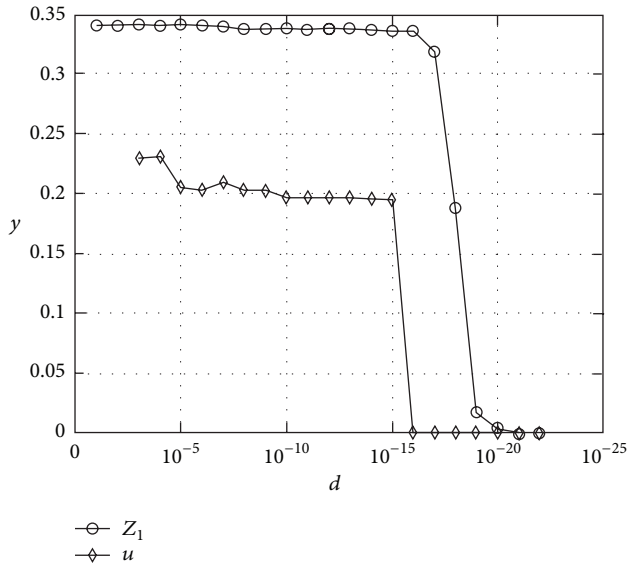


Figure 1: The value spaces of Z_1 and u.

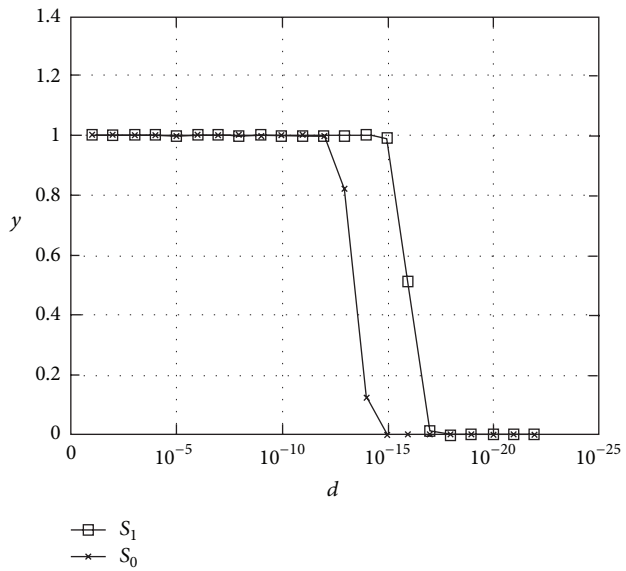


Figure 2: Value spaces of S_1 and S_0.

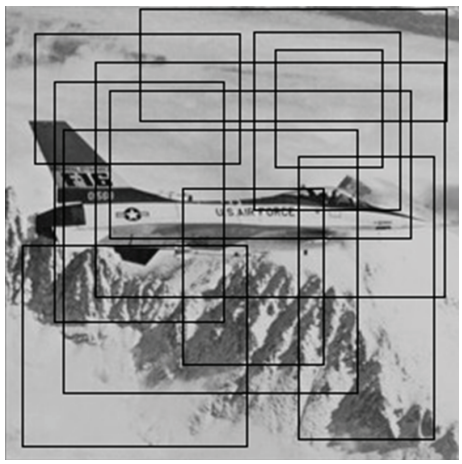


Figure 3: Image divided randomly into overlapping blocks.

2.2. Robust Local Feature Points Based on Gravity Center of Random Blocks. The local features of the image should be not only stable under geometric transforms such as rotation and scaling but also robust to insignificant distortions such as additive noising and blurring, bit errors, and packet losses during transmission in WMSNs. Based on the image random blocking in Section 2.1, we propose a robust local feature points extraction method using the gravity center of random blocks. The extracted robust local features will then be used to generate perceptual hashes in Section 2.3.

The two-dimensional (2D) moment can be directly used in the interested regions and does not need to separate them from the whole image. High-order moments are more sensitive to noise, while the low-order moments are insensitive to noise and bit errors, which is beneficial to the characterization of collectivity for the regions.

The 2D $(p + q)$th order origin moment of a continuous image I is defined as [18]

$$M_{pq} = \int_I x^p y^q f(x, y)\, dx\, dy, \qquad p, q = 0, 1, 2, \ldots, \tag{9}$$

where $f(x, y)$ represents the gray-level value at location (x, y). For digital image the integrals are replaced by summations and M_{pq} becomes

$$M_{pq} = \sum_{(x,y)\in I} x^p y^q f(x, y), \qquad p, q = 0, 1, 2, \ldots. \tag{10}$$

The gravity center $G(m_x, m_y)$ of the image is defined in terms of the zero-order moment and first-order moments as follows:

$$m_x = \frac{M_{10}}{M_{00}}, \qquad m_y = \frac{M_{01}}{M_{00}}, \tag{11}$$

where the zero-order moment M_{00} represents the area of the image clearly.

In order to obtain the local feature, the coordinate of the gravity center $G_k(m_x^k, m_y^k)$ of each random rectangular block is calculated as

$$\begin{aligned} m_x^k &= \frac{\sum_x \sum_y x \cdot f^k(x, y)}{\sum_x \sum_y f^k(x, y)}, \\ m_y^k &= \frac{\sum_x \sum_y y \cdot f^k(x, y)}{\sum_x \sum_y f^k(x, y)}, \\ k &= 1, 2, \ldots, C, \end{aligned} \tag{12}$$

where $f^k(x, y)$ represents the gray-level value at location (x, y) in the kth random rectangular block and C is the number of random rectangular blocks. Thus, there are total C gravity centers of the pseudorandom rectangular blocks denoted by $G = \{G_1, G_2, \ldots, G_k, \ldots, G_C\}$. The local feature information of the image can be obtained by calculation of each block's gravity center, which improves the ability to distinguish different images.

The gravity center of the image has geometrically invariant property. In this paper, the rotation invariability is analyzed as an example. After a rotation by an angle θ about the original, the first-order moments are given by

$$\begin{aligned} M_{10}^r &= \sum_{(x,y)\in\Omega} (x\cos\theta + y\sin\theta) f(x, y) \\ &= M_{10}\cos\theta + M_{01}\sin\theta, \\ M_{01}^r &= \sum_{(x,y)\in\Omega} (y\cos\theta - x\sin\theta) f(x, y) \\ &= M_{01}\cos\theta - M_{10}\sin\theta \end{aligned} \tag{13}$$

and the zero-order moment $M_{00}^r = M_{00}$. So after a rotation by an angle θ, the changed gravity center is

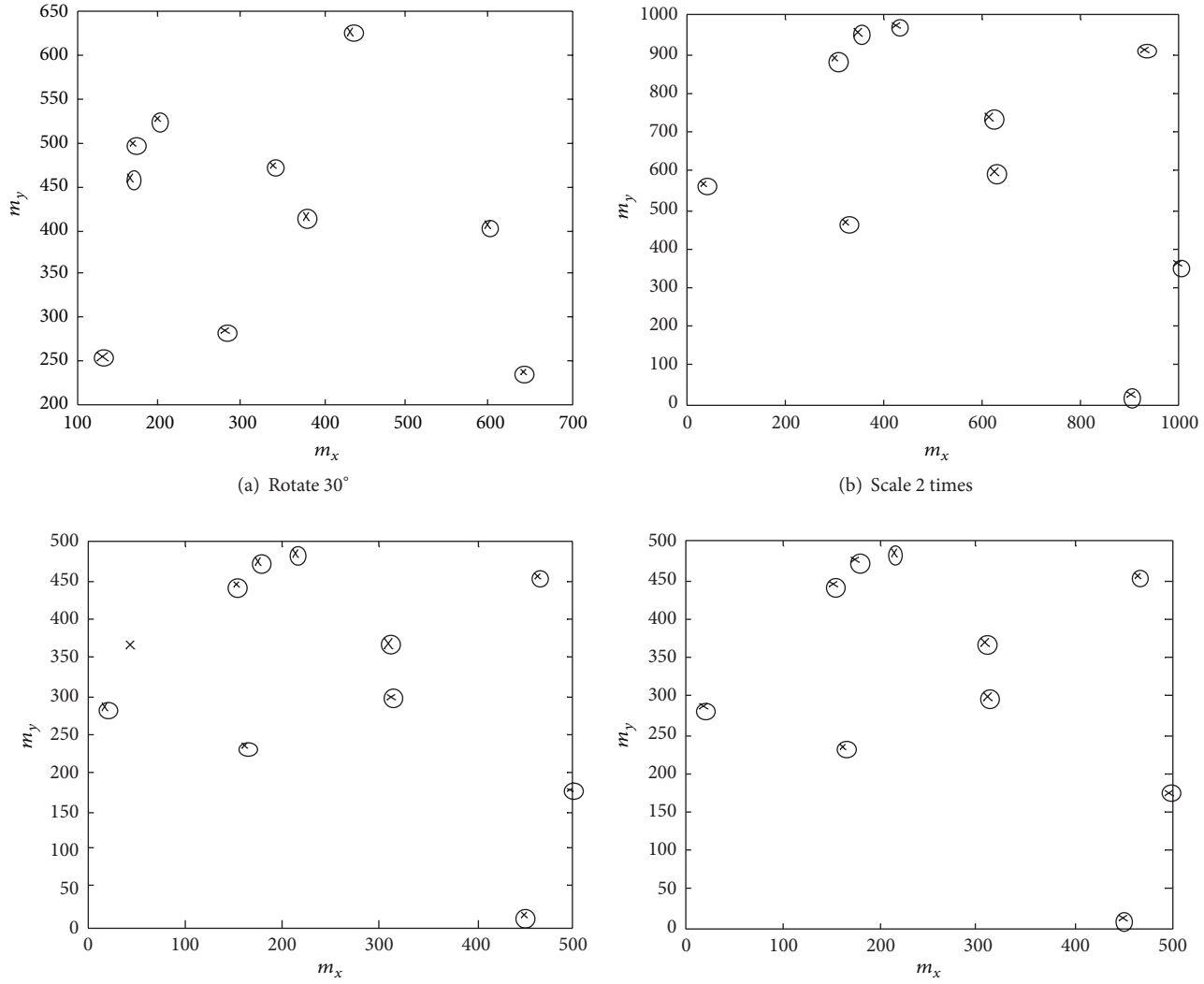
$$\begin{aligned} G_x^r &= \frac{M_{10}^r}{M_{00}^r} = G_x\cos\theta + G_y\sin\theta, \\ G_y^r &= \frac{M_{01}^r}{M_{00}^r} = G_y\cos\theta - G_x\sin\theta. \end{aligned} \tag{14}$$

Namely,

$$\begin{bmatrix} G_x^r \\ G_y^r \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} G_x \\ G_y \end{bmatrix}. \tag{15}$$

Thus, the rotation invariability is held. In similar analysis, other geometrical invariability characteristics can also be obtained.

Figure 4 shows the robustness of gravity centers under geometric distortions and common image processing. Note that × denotes the virtual locations gravity centers in the distorted image and o denotes theoretical locations of gravity centers. Once the two symbols are coincident, the geometrical invariability of gravity centers and the strong robustness to additive noise and JPEG compression will be indicated.



(a) Rotate 30°

(b) Scale 2 times

(c) Additive white Gaussian noise (variance is 46)

(d) JPEG compression (quality factor is 50%)

Figure 4: Robustness of gravity centers under geometric distortions and common image processing.

2.3. Perceptual Image Hashes Generation. The supplement image block of each random rectangular block is defined as

$$\widetilde{f}(x, y) = R_{\text{level}} - f(x, y), \tag{16}$$

where R_{level} is the maximum gray-scale level of the image. Likewise, we obtain the gravity center of the supplement image block. For each rectangular block, we calculate its supplement image block's gravity center and obtain total C gravity centers of the supplement image blocks. The normal gravity center of image usually lies around the center of image, so does that of the supplementary image. Thus the distance between the two gravity centers of image and its supplement image is short. We devise a solution by making a modification of the gravity center. The improved supplement image blocks' gravity center $\widehat{G}^k(\widehat{m}_x, \widehat{m}_y)$ of kth rectangular image block is obtained by

$$\begin{aligned} \widehat{m}_x^k &= \frac{\sum_x \sum_y x \cdot \exp\left(f^k(x, y)/\Delta_1\right)}{\sum_x \sum_y \exp\left(f^k(x, y)/\Delta_1\right)}, \\ \widehat{m}_y^k &= \frac{\sum_x \sum_y y \cdot \exp\left(f^k(x, y)/\Delta_1\right)}{\sum_x \sum_y \exp\left(f^k(x, y)/\Delta_1\right)}, \end{aligned} \tag{17}$$

where $\Delta_1 > 0$ is the quantification step. Through such modification, we enlarge the distance between the two gravity centers on one hand. On the other hand, the parameter Δ_1 guarantees the robustness against malicious attacks in calculating the two gravity centers.

In order to generate the perceptual image hashes, we calculate the distance of the two gravity centers between each rectangular block and its supplement image block. Considering the constraints on limited energy and computing

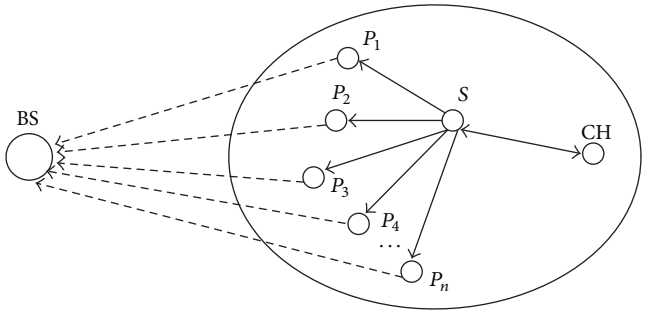


Figure 5: Structure of clustering in WMSNs.

resources in WMSNs, we use L_∞ norm to measure the spatial distance D_k between the locations of the two gravity centers for each rectangular block as follows:

$$D_k\left(G_k, \widehat{G}_k\right) = \max\left\{\left|m_x^k - \widehat{m}_x^k\right|, \left|m_y^k - \widehat{m}_y^k\right|\right\}, \quad k = 1, 2, \ldots, C. \tag{18}$$

Let $\Delta_2 > 0$ be another quantification step, and the distance D_k between the two gravity centers can be quantified as

$$\overline{D}_k = \left\lfloor \frac{D_k}{\Delta_2} \right\rfloor \Delta_2, \tag{19}$$

where $\lfloor \cdot \rfloor$ denotes the floor function. Obviously, the quantified distance $\overline{D}_k$ will be decimal integer. Moreover, the distance $\overline{D}_k$ is more robust against common image processing and the bit errors during transmission.

Then, we convert the decimal $\overline{D}_k$ to binary sequence $(b_{k,1}, b_{k,2}, \ldots, b_{k,j})_2$, $b_{k,j} \in \{0, 1\}$, and finally combine the binary sequences of each distance together to form the perceptual hashing sequence H as follows:

$$\begin{aligned} H = {} & \left(b_{1,1}b_{1,2}\cdots b_{1,j}\right)_2 \left\|\left(b_{2,1}b_{2,2}\cdots b_{1,j}\right)_2\right\| \cdots \\ & \left\|\left(b_{k,1}b_{k,2}\cdots b_{k,j}\right)_2\right\| \cdots \left\|\left(b_{C,1}b_{C,2}\cdots b_{C,j}\right)_2\right. . \end{aligned} \tag{20}$$

3. Distributed Processing Strategy for Perceptual Image Hashes

In WSNs, clustering expedites many desirable functions and provides many advantages such as load balancing, energy savings, and distributed key management. The most prominent benefit of clustering is that it can greatly reduce the energy consumption of nodes and lengthen the network lifetime [19]. In this paper, in order to adapt well to the limited power resources and computational capabilities in sensor nodes, we consider clustering-based WMSNs with densely distributed nodes. The structure of a clustering is shown in Figure 5. Each clustering consists of a cluster head (CH), several general cluster member nodes, and a camera sensor that captures the digital image. In Figure 5, *BS* represents the base station, CH is a cluster head node, *S* is the image capturing node, and $P_1 \sim P_n$ are the general cluster member nodes whose each node is assigned a fixed ID.

The distributed processing strategy is as follows:

Step 1. The cluster head node CH generates a secure pseudo-random chaotic sequence with the keys k_1 and k_2 according to the method in Section 2.1 and sends this chaotic sequence to the image capturing node *S*. In addition, the ID of each general cluster member node P_i $(i = 1, 2, \ldots, n)$ is also sent to node *S*.

Step 2. When the image capturing node *S* captures an image, it will use the received chaotic sequence to divide randomly the captured image into C overlapping rectangles. Moreover, each rectangle block is sent to the general cluster member node P_i. Note that the chaotic sequence is mapping to the ID of the general cluster member nodes one by one.

Step 3. The distance of the two gravity centers for each rectangle block will be calculated in each general cluster member node P_i, and its corresponding binary sequence $(b_{k,1}, b_{k,2}, \ldots, b_{k,j})_2$ can be generated by the method in Section 2.3, which is sent to the cluster head node CH.

Step 4. The cluster head node CH receives the binary sequences $(b_{k,1}, b_{k,2}, \ldots, b_{k,j})_2$, $k = 1, 2, \ldots, C$, from all of the general cluster member nodes, then combines them to form the perceptual hashing sequence, and finally the cluster head node CH sends the perceptual hashing sequence to the base station for image authentication purpose.

4. Perceptual Hashing-Based Image Authentication

When we identify the received image, firstly, the perceptual hashing sequence is obtained from the base station and is matched with the perceptual hashing sequence generated by the dubitable image. If the Hamming distance between two perceptual hashing sequences is less than the specified threshold, the image will be deemed an authentic version. Otherwise, the image is forged.

The image authentication framework is shown in Figure 6. The steps are as follows.

Step 1. The perceptual hashing sequence H_1 is received from the base station.

Step 2. The dubitable image is partitioned into C random rectangular blocks by the same secret keys k_1 and k_2 like perceptual hashing generation process described in Section 2.1; then the distance of the two gravity centers for each rectangle block is calculated and quantified; after that the robust feature is extracted. Thus another perceptual hashing sequence H_2 can be restructured like the description in Section 2.3.

Step 3. Setting a threshold $T > 0$, normalized Hamming distance is calculated by

$$DH\left(H_1, H_2\right) = \frac{1}{L}\sum_{k=1}^{L}\left|H_1(k) - H_2(k)\right|, \tag{21}$$

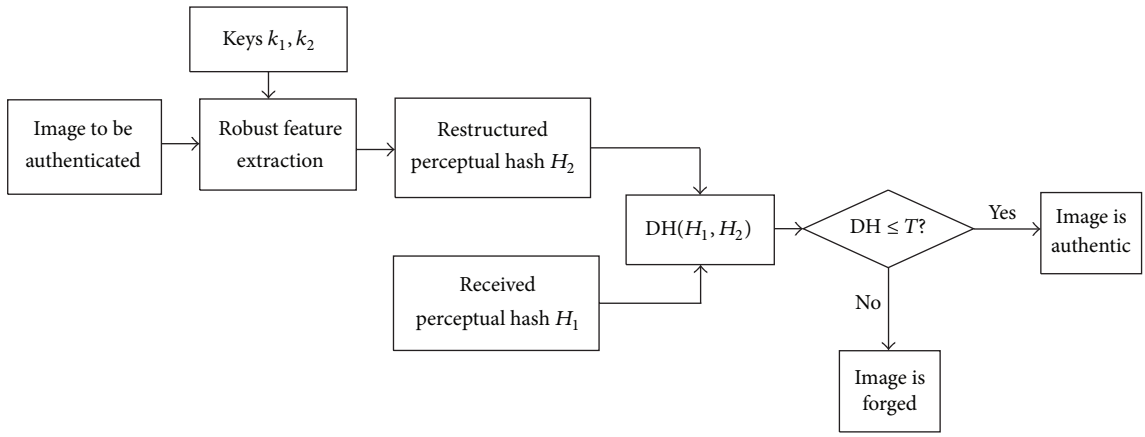


Figure 6: Image authentication process.

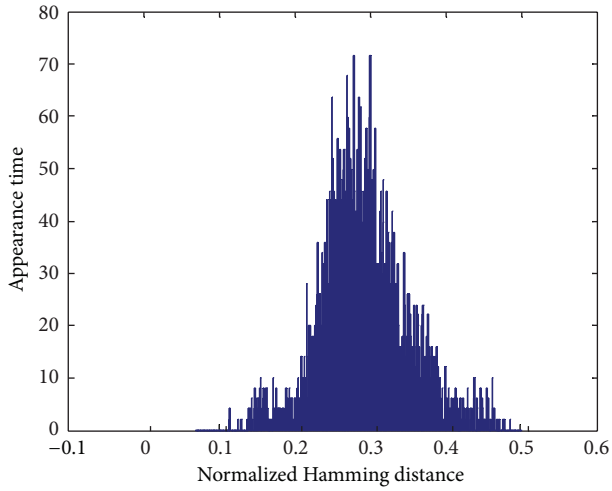


Figure 7: Visual fragility test.

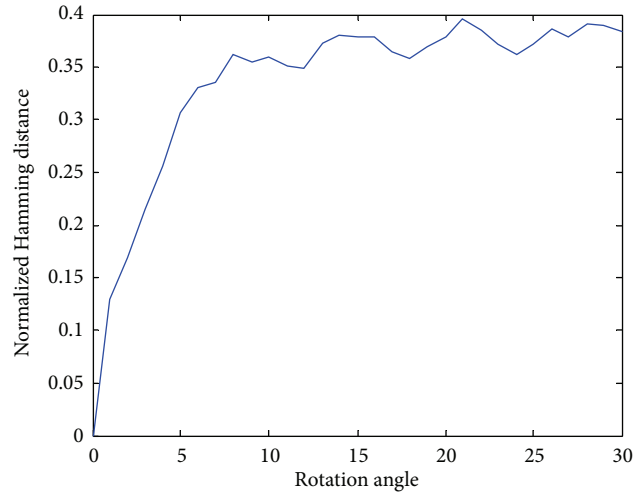


Figure 8: Robustness to image rotation.

where L is the length of perceptual Hashing sequence. If $DH(H_1, H_2) \leq T$, the image will be deemed an authentic version. Otherwise, if $DH(H_1, H_2) > T$, the image will be forged. The smaller the normalized Hamming distance is, the stronger the robustness is. Ideally, the normalized Hamming distance for the perceptually identical images is close to 0, while the normalized Hamming distance of two different images is close to 0.5.

5. Experimental Results and Analysis

5.1. Visual Fragility of Perceptual Hashes. The visual fragility represents that perceptually distinct images generate different perceptual hashes. We randomly select 80 images sized 300×300. The parameters are set as follows: $k_1 = 3.9$, $k_2 = 1.2$, $\Delta_1 = 10$, $\Delta_2 = 4$, and the number of random rectangle blocks is 150. Then we calculate their perceptual hashes and the Hamming distance between two perceptual hashing values $DH(H_1, H_2)$. Finally, 6320 matching results can be obtained. The statistical histogram distribution is shown in Figure 7. From Figure 7, we see the results can be approximate to the Gaussian distribution with the expectation $\mu = 0.2924$ and standard deviation $\sigma = 0.0574$. Setting the threshold $T = 0.125$, the conflict probability will be

$$P_c = 1 - \int_T^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-(x-\mu)^2/2\sigma^2} dx = 2.8106 \times 10^{-6}. \quad (22)$$

As a result, the conflict probability is very small. Hence, the proposed perceptual hashing can ensure the visual fragility.

5.2. Perceptual Robustness. To test the perceptual robustness to geometric transforms, we rotate the "Lena" image sized 512×512 with different degrees and calculate the perceptual hashes. Compare the perceptual hashing value of rotated image with the original. The relationship of the rotation angle and the normalized Hamming distance is shown in Figure 8. When the image rotation angle is within 5°, the normalized Hamming distance is less than 0.3, so the proposed perceptual hashing algorithm is robust to image rotation within 5°.

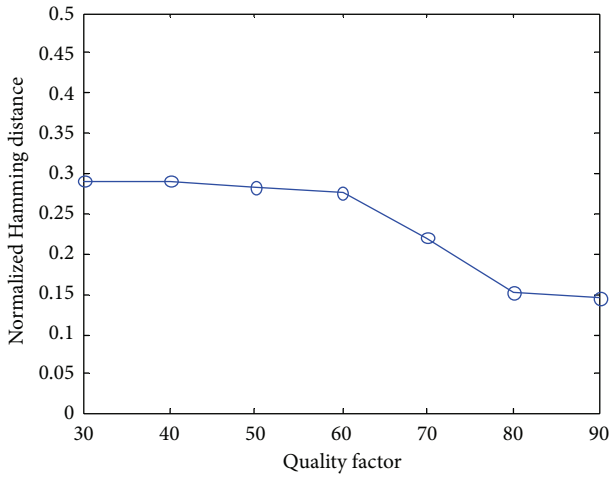


Figure 9: Robustness to image compression.

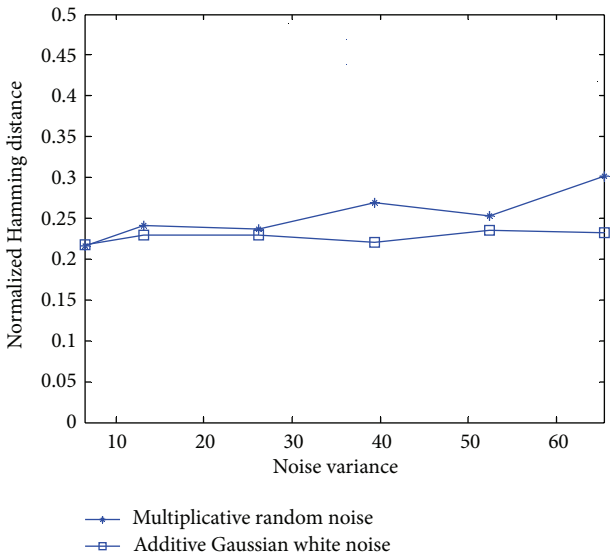


Figure 10: Robustness to noise blurring.

Figure 9 shows the robustness to image compression. When the quality factor of JPEG compression is changed from 90 to 30, the normalized Hamming distance between the original image and the compressed image is less than 0.3, so the proposed perceptual hashing algorithm is robust to image compression. The smaller the quality factor is, the larger the compression degree is. From Figure 9, we see that the robustness is getting more and more strong with the accretion of the quality factor.

Figure 10 shows the robustness to additive Gaussian white noise and uniformly distributed multiplicative random noise. When the image is blurred by different noise degrees with variance 6.554 $\sim$ 65.54, we calculate the perceptual hashes. From Figure 10, we see that, when the variance is less than 65.54, the normalized Hamming distance between the original image and the noise blurred image is less than 0.3; That is to say, the proposed algorithm is robust to Gaussian white noise and uniformly distributed random multiplicative noise during image transmission and storage.

Table 1: Perceptual hashing segments by different keys.

Segment 1 ($k_1 = 3.9, k_2 = 1.2$)	$\cdots$1001011100011011000011010000$\cdots$
Segment 2 ($k_1 = 3.91, k_2 = 1.2$)	$\cdots$1000110110010100100110000100$\cdots$
Segment 3 ($k_1 = 3.9, k_2 = 1.21$)	$\cdots$1010100110001001110010011110$\cdots$

5.3. Security. Because the chaotic sequence is nonperiodic and sensitive to the initial value, the chaotic maps (6) and (7) are used to generate the pseudorandom sequence in this paper. Then, the digital image is randomly divided into overlapping rectangular regions by the chaotic sequence for perceptual image hashing extraction. Thus, if chaotic initial values are changed, that is, the keys are different, the extracted perceptual image hashing will be different. Table 1 lists the segments of the generated perceptual image hashes by different keys, which indicates the perceptual hashing is intractable without the secret key. We can calculate that the normalized Hamming distance is 0.4167 between the corresponding locations of the perceptual hashing segment 1 and segment 2 and that it is 0.4283 between segment 1 and segment 3. The two normalized Hamming distances are all close to 0.5, so the security meets the application requirement. Therefore, without knowing the key, even if the perceptual image hashing algorithm is known, the correct perceptual hashing value generated by the image cannot be leaked.

6. Conclusions

In this paper, we have proposed a robust image authentication methodology for authenticity, creditability, and integrity transmission and storage of authenticated images based on the perceptual hashing technique in WMSNs. First, a gravity center-based perceptual image hashing algorithm is proposed with compactness, perceptual robustness, visual fragility, and security. The generated perceptual hashing value is a short binary string as a digest of the image in order to tackle the problem of severe energy constraints and perceptual image redundancy in WMSNs. Furthermore, a distributed processing strategy for perceptual image hashes is developed to meet the limited computing resources of sensor nodes in WMSNs. The experimental results demonstrate that our scheme has the satisfactory authentication performance for perceptually distinct and identical images.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (NSFC) under Grant no. 61170226, the Fundamental Research Funds for the Central Universities under Grants nos. SWJTU11CX047, SWJTU12ZT02, the Young Innovative Research Team of Sichuan Province under Grant no. 2011JTD0007, and Chengdu Science and Technology program under Grant no. 12DXYB214JH-002.

References

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdury, "Wireless multimedia sensor networks: a survey," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 32–39, 2007.

[2] H. Wang, M. Hempel, D. Peng, W. Wang, H. Sharif, and H. H. Chen, "Index-based selective audio encryption for wireless multimedia sensor networks," *IEEE Transactions on Multimedia*, vol. 12, no. 3, pp. 215–223, 2010.

[3] Y. Y. Zhang, X. Z. Li, J. M. Liu, J. C. Yang, and B. J. Cui, "A secure hierarchical key management scheme in wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 547471, 8 pages, 2012.

[4] S. Han, E. Chang, L. Gao, and D. Tharam, "Taxonomy of attacks on wireless sensor networks," in *Proceedings of the 1st European Conference on Computer Network Defense*, pp. 97–105, Glamorgan, UK, December 2005.

[5] S. G. Yoo, K. Y. Park, and J. Kim, "A security-performance-balanced user authentication scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 382810, 11 pages, 2012.

[6] B. Harjito and S. Han, "Wireless multimedia sensor networks applications and security challenges," in *Proceedings of the 5th International Conference on Broadband Wireless Computing, Communication and Applications (BWCCA '10)*, pp. 842–846, November 2010.

[7] M. K. Khan, "Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world," *IETE Technical Review*, vol. 26, no. 3, pp. 191–195, 2009.

[8] Z. Li, Q. Sun, Y. Lian, and C. W. Chen, "Joint source-channel-authentication resource allocation and unequal authenticity protection for multimedia over wireless networks," *IEEE Transactions on Multimedia*, vol. 9, no. 4, pp. 837–850, 2007.

[9] W. Wang, D. Peng, H. Wang, H. Sharif, and H. H. Chen, "Energy-distortion-authentication optimized resource allocation for secure wireless image streaming," in *Proceedings of the IEEE Conference on Wireless Communications and Networking (WCNC '08)*, pp. 2810–2815, April 2008.

[10] Z. Zhang, Q. Sun, W. C. Wong, J. Apostolopoulos, and S. Wee, "An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks," *IEEE Transactions on Multimedia*, vol. 9, no. 2, pp. 320–331, 2007.

[11] W. Wang, D. Peng, H. Wang, H. Sharif, and H. H. Chen, "A multimedia quality-driven network resource management architecture for wireless sensor networks with stream authentication," *IEEE Transactions on Multimedia*, vol. 12, no. 5, pp. 439–447, 2010.

[12] Z. Zhang, Q. Sun, W. C. Wong, J. Apostolopoulos, and S. Wee, "Rate-distortion-authentication optimized streaming of authenticated video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 5, pp. 544–557, 2007.

[13] Q. Sun and S. F. Chang, "A secure and robust digital signature scheme for JPEG2000 image authentication," *IEEE Transactions on Multimedia*, vol. 7, no. 3, pp. 480–494, 2005.

[14] Q. Sun, D. He, and Q. Tian, "A secure and robust authentication scheme for video transcoding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 10, pp. 1232–1244, 2006.

[15] D. Skraparlis, "Design of an efficient authentication method for modern image and video," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 417–426, 2003.

[16] X. D. Lv and Z. J. Wang, "Perceptual image hashing based on shape contexts and local feature points," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1081–1093, 2012.

[17] M. Tagliasacchi, G. Valenzise, and S. Tubaro, "Hash-based identification of sparse image tampering," *IEEE Transactions on Image Processing*, vol. 18, no. 11, pp. 2491–2504, 2009.

[18] K. R. Castleman, *Digital Image Processing*, Prentice Hall, New York, NY, USA, 1998.

[19] G. Wang, D. Kim, and G. Cho, "A secure cluster formation scheme in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 301750, 14 pages, 2012.