http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

OPEN ACCESS Information Technology Journal

ISSN 1812-5638
DOI: 10.3923/itj.2016.10.17

Research Article
Dual Water Marking Based Image Collection in Multimedia Sensor Networks

[1]Hai Huang, [2]Dong-Qing Xie and [2]Ke Qi

[1]School of Mathematics and Information, Guangzhou University, 230 Waihuan West Road, Guangzhou Higher Education Mega Center, Guangzhou, China
[2]School of Computer Science, Guangzhou University, China

Abstract
This study presents a novel image collection scheme for multimedia sensor networks based on dual water marking. The dual water marking includes two folds: one is robust water mark for the identification of the sender and freshness authentication of images and the other is the fragile water mark for the tamper detection and recovery of image contents. In this scheme, the sensor node groups image frames and two successive frames compose the non-overlapping authentication and restoration group. The dual water marking bits are computed from the first image and embedded into the image group. The sink performs the verification and recovery by dual water mark. Compared with previous work, our approach can not only implement the task of identification and authentication, but also improve image quality. Experimental results show that our scheme achieves significant gains in terms of identification and authentication performance and efficient packet loss tolerance to improve the image quality.

Key words: Multimedia sensor networks, image recovery, identification and authentication, dual water marking

Received: June 10, 2015 Accepted: September 08, 2015 Published: December 15, 2015

Citation: Hai Huang, Dong-Qing Xie and Ke Qi, 2016. Dual Water Marking Based Image Collection in Multimedia Sensor Networks. Inform. Technol. J., 15: 10-17.

Corresponding Author: Dong-Qing Xie, School of Computer Science, Guangzhou University, 230 Waihuan West Road, Guangzhou Higher Education Mega Center, Guangzhou, China

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

The identification of the sender and freshness authentication of the sensory image data and high image quality is the core requirement for Multimedia Sensor Networks (MSNs). However, due to the limited computational capacity, storage space and energy, traditional solutions for identification and authentication based on cryptography and image quality mechanism are often unsuitable for MSNs (Zhu *et al*., 2006; Karlof *et al*., 2004).

Some previous works (Kamel and Juma, 2010, 2011) proposed the authentication schemes for Wireless Sensor Networks (WSNs) based on digital water marking. Water marking is much lighter than cryptographic algorithms and brings no additional payload. However, the embedded water mark for these schemes can only complete data integrity or copyright protection, but can't do the identification of the sender and freshness authentication of the image, which is one of the foundational requirements for applications in MSNs.

The high Quality of Service (QoS) is the other requirement for applications in Multimedia Sensor Networks (MSNs). However, due to the channel instability and limited node resources which result in congestion and packet loss, traditional solutions for reliable image transmission based on error controlling and retransmission are also not suitable for Multimedia Sensor Networks (MSNs).

This study proposes a novel secure image collection scheme with efficient packet loss tolerance in MSNs based on frame group and dual water marking. The proposed scheme can verify the identification of the sender and freshness authentication of the sensory image through the embedded dual water marking image and can restore the damaged parts of original image to improve the image quality. It fulfills the secure image collection demand of both authentication and image recovery in Multimedia Sensor Networks (MSNs).

The LEAP (Zhu *et al*., 2006) is designed to support in network processing and to restrict the security impact of nodes in the immediate neighborhood of the compromised node. However, LEAP suffers from with high processing and communication cost. TinySec (Karlof *et al*., 2004) is the first fully-implemented link layer security protocol for WSNs, which provides data confidentiality and integrity authentication. TinySec computes a four-byte Message Authentication Code (MAC) which is attached to the packet. TinySec is carefully designed to achieve a balance between constrained resource and security, but it still introduces additional communication overhead. The above security scheme for WSNs is based on cryptographic algorithms, which employ expensive expensive operations. Therefore, the mentioned scheme is not suitable for WSNs.

Water marking is used for authentication through embedding water mark into original data. Kamel and Juma (2010) proposed the light weight chained water marking (LWS) scheme, which uses a fragile chaining water marking scheme to verify and locate modification to the data. Kamel and Juma (2011) proposed a light weight forward chaining water marking scheme named FWS-D, which organizes data into groups of constant sizes. Hash function is only used to generate water mark through a group and water mark is embedded into the previous group to form a forward-chaining. These water mark based authentication schemes uses irreversible water mark which is unable to restore the original data completely. The packet loss in the transmission of MSNs produces many damaged blocks in images and leads to low image quality. Some related works of Sun *et al*. (1997), Hemami and Meng (1995), Wu and Abouzeid (2006) and Chen *et al*. (2007) have been proposed to improve image quality in MSNs which use transmission error controlling and multipath routing. Sun *et al*. (1997) and Hemami and Meng (1995) proposed the image restoration scheme which implements blind restoration in sink. Wu and Abouzeid (2006) used both multipath routing and Reed-Solomon error correction to improve the image quality. Chen *et al*. (2007) proposed the scheme which combines forward error controlling code with multipath routing based on direction graphic routing to provide reliable transmission. However, the additional error controlling code results in additional communication costs and cannot tolerate packet loss.

MATERIALS AND METHODS

Dual image water marking: The dual image water marking includes the spatial fragile water mark and the frequency robust water mark. Firstly, the frequency robust water mark with the water mark bits of identity and timestamp is embedded and then the spatial fragile water mark with the water mark bits of image content is embedded.

Robust water mark embedding: The robust water mark bits are embedded into the DWT coefficients of the image. Let w ($w \in \{0,1\}$) be the water mark bits. The LSB of the $N \times N$ image is set to zero firstly and then is decomposed into two-level DWT and the water mark bits is embedded into the HH2 sub-band. The HH2 coefficients are divided into 2×2 non-overlapped sub-block C and the water mark bits w are embedded as following:

$$\begin{cases} C(1,1) = \min\ (C(1,1), C(1,2), C(2,1), C(2,2)) - T, \ w = 1 \\ C(1,1) = \max\ (C(1,1), C(1,2), C(2,1), C(2,2)) + T, \ w = 0 \end{cases}$$

where, T is the embedding strength. After all sub-block finished the embedding, the water marked image is recovered by inverse DWT.

Fragile water mark embedding: The fragile water mark bits are embedded into the LSB of the processed image. In order to generate water mark bits based on image content, the robust water marked N×N image is divided into 2×2 non-overlapped sub-block and the first pixel of each sub-block is picked up to construct the approximate image which has a quarter size of the original image. The highest four bit planes of the approximate image are extracted to generate N×N binary water mark bits w and then the water mark bits w are embedded into the LSB of the image.

Since the water marks bits which contain the image content can be used to recover the damaged original image, we adapt its main idea for tamper location and image restoration in MSNs.

Dual water mark extraction: The dual water mark extraction has two steps:

Step 1: The robust water mark is extracted. The LSB of dual water marked image is set to zero and is decomposed into two-level DWT. The HH2 coefficients are divided into 2×2 non-overlapped sub-block C′. For each sub-block C′, let s = (C′(1, 2)+C′(2, 1)+C′ (2,2))/3, the water mark bit w′ is extracted as following: w′=1 if C′(1,1)$\leq$s and w′=0 if C′(1,1)$\geq$s. After all sub-blocks finished the extraction, the water mark bits are obtained

Step 2: The fragile water mark is extracted. The LSB of water marked image is extracted to obtain the N×N binary water mark bits w′. In order of tamper location and image recovery, w′ is decomposed as the same order of the embedding to obtain the four bit planes. The tamper location can then be done by comparing the higher four bit planes of the image with obtained four bit planes and image recovery can also be done by substituting the obtained four bit planes for the responding tampered pixels according to the tamper location

Proposed scheme

System model: We consider the image collection model of MSNs (Fig. 1) that consists of three types of nodes: The image sensor node, the cluster node and the sink node. Sensor nodes periodically report their sensory image to the storage node. Sensory image from each sampling is available as an element of the image stream. The water mark bits are generated from the original image and contain the image content and embedded in the sensor node. The cluster node just transmutes the water marked image to the sink node. The sink node verifies and restores the responding images. In other word, the sensor node is the encoder in which data is buffered and manipulated; the sink is the decoder, verifier and recover; and the cluster node does nothing but transmission.

The sensor node sets two adjacent images as a group, which composes the non-overlapping authentication and recovery group. The robust water mark bits are computed from the identity and timestamp and embedded into the first image itself and the fragile water mark bits are computed from the first image and embedded into the second one before transmission. In the other end, sink queries the image group,

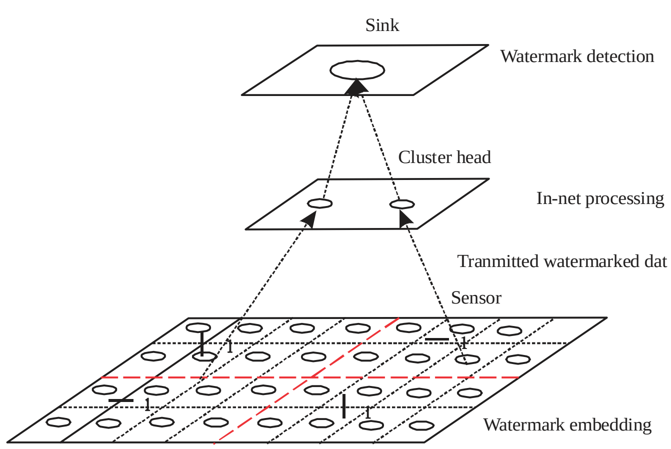

Fig. 1: MSNs model

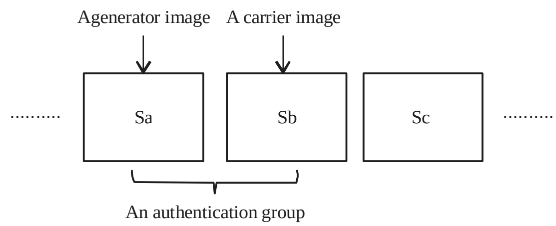

Fig. 2: Example of group

authenticates the image by robust water mark and then recovers the original image by fragile water mark.

Grouping: As shown in Fig. 2, s_a, s_b, s_c are three successive images. Two adjacent images compose an authentication group, e.g., {s_a, s_b} or {s_b, s_c}. The water mark is generated from the first image and embedded into the second image, so the two images are called generator image and carrier image.

Dual water mark generation and embedding: The dual water mark generation and embedding is group-based.

In terms of sender identification and freshness authentication, the robust water mark should contain the identity of the sensory node and timestamp of the collected image. Let N×N image S_a be the generator image (Fig. 2), the node ID and timestamp are just linked to generate water mark bits (w_{r1} w_{r2} w_{r3}.. w_{rL}) ($w \in \{0,1\}$).

In terms of image recovery depending on embedded water mark, the fragile water mark should contain as much image information as possible. Let N×N image S_a be the generator image (Fig. 2), we divided the generator image S_a into 2×2 non-overlapped sub-block, the first pixel of each sub-block is then picked up to construct the approximate image b with a quarter size of S_a. The highest four bit planes of the approximate image are extracted to generate N×N binary bits and the N×N binary bits (w_{f1} w_{f2} w_{f3}.., w_{fL}) (L = N×N, $w \in \{0,1\}$) are the candidates of water mark bits which contain the pixel information of the generator image. Pseudo code for the fragile water mark generating algorithms is presented in Algorithm 1.

After the generation of the dual water mark bits, we apply the dual water mark embedding, which is similar with the image water marking algorithm described in the Section. It's notable that the robust water mark bits is embedded into the generator image S_a and the fragile water mark bits is embedded into the carrier image S_b (Fig. 2).

Both the water mark generation and embedding require only the current image and the previous results rather than the whole group. So, the sensor node only needs to buffer one image, i.e., the current one, which is denoted as buffer image (S_b). After the completion of the current image processing, the sensor node clears the image buffer, which is denoted as buffer image clear (S_b).

Pseudo code for the dual water mark embedding algorithms is summarized in Algorithm 2.

Algorithm 1: Fragile water mark generating

```
2×2 non-overlapped sub-block division of generator image Sa
w = null
For each sub-block C
s = get Pixel (C (1,1));//Get the first pixel of the sub-block
w1 = MSB (s);//Get the MSB of the pixel
w2 = 2SB (s);//Get the seventh bit of the pixel
w3 = 3SB (s);//Get the sixth bit of the pixel
w4 = 4SB (s);//Get the fifth bit of the pixel
w = w||w1||w2||w3||w4;//link four bits to generate water mark bits
End
```

Algorithm 2: Dual water mark embedding

```
Input robust water mark (wr1 wr2 wrj. . wrL)
Buffer Image (Sa)
LSB (Sa) = 0;
(HH1, HL1, LH1, HH2, HL2, LH2, LL2) = DWT2 (Sa);// 2-level DWT of Sa
(C1, C2,..., Cj,...Cn) = Partition (HH2)
//Partite HH2 into 2×2 sub-block
For each sub-block Cj
If (wrj = = 1)
C (1,1) = min (C (1,1),C (1,2),C (2,1),C (2,2))-T;
End
If (wrj = = 0)
C (1,1) = max (C (1,1),C (1,2),C (2,1),C (2,2))+T;
End
End
S'a = IDWT2 ( (HH1, HL1, LH1, HH2', HL2, LH2, LL2))
//2-level IDWT to recover the robust water marked image
(wf1 wf2 wf3. . wfL) = fragile water mark generating (Sa)
Buffer image clear (Sa)
Buffer image (Sb)
S'b = LSB Embedding (Sb, (wf1 wf2 wf3. . wfL));//LSB embedding of Sb
Buffer image clear (Sb)
```

Authentication: It is reasonable to assume that the resource and energy of the sink is not as strictly constrained as the sensor. When the sink queries the dual water marked image, the successive images are responded to the sink node. When the dual water marked images arrive, the sink groups the images in the same way and buffers at least one group before processing, which is denoted as Buffer group (S). The sink extracts the robust water mark w_r = (w_{r1} w_{r2} w_{r3}.. w_{rL}) from the first image of the group, the extraction is similar with the water mark extraction algorithm described in section. Since w_r contain the node ID and time stamp and the sink preserves the past communication log, the sink can verify the w'_r with preserved node ID and timestamp to determine the identification of the sender and freshness authentication of the image.

If the water mark verification succeeds, the generator image will be marked authenticated. If the water mark verification fails, the generator image will be marked unauthenticated. After authentication, the generator image will be empty and the carrier image should be kept in buffer.

When the next image appears, a new authentication group will be composed by the buffered carrier image and the newly arrived image.

Pseudo code for the authentication algorithms is summarized in Algorithm 3.

Tamper location and image recovery: After successful water mark verification, we can use the fragile water mark extracted from the second image S_b to tamper location and recover the lost parts of image S_a which may be caused by the pocket loss.

The LSB of image S_b is extracted to obtain the N×N binary water mark bits $w_f = (w_{f1}\ w_{f2}\ w_{f3}..\ w_{fL})$ (L = N×N) and then we use w_f to tamper location and image recovery with the water mark extraction algorithm described in section. Pseudo code for the tamper location and image recovery algorithms is summarized in Algorithm 4.

Algorithm 3: Authentication

(S'_a, S'_b) = Buffer Group (S);
LSB (S'_a) = 0;
(HH1, HL1, LH1, HH2, HL2, LH2, LL2) = DWT2 (S'_a);// 2-level DWT of S'_a
$(C'_1, C'_2, \cdots, C'_j, \cdots, C'_n)$ = Partition (HH2);
//Partite HH2 into 2×2 sub-block
For each sub-block C'_j
s = (C'_j (1,2)+C'_j (2,1)+C'_j (2,2))/3;
If C'_j (1,1)≤s
$w'_j = 0$
End
If C'_j (1,1) ≥s
$w'_j = 1$
End
End
$w_r = (w'_{r1}\ w'_{r2}\ w'_j..\ w'_{rL})$;
w' = code (ID, time stamp);//coding preserved node ID and timestamp
Verify (w', w'_r);//verify identification and freshness

Algorithm 4: Tamper location and image recovery

$(w_{f1}\ w_{f2}\ w_{f3}..\ w_{fL})$ = LSB (S'_b)
Four bit planes = decompose $(w_{f1}\ w_{f2}\ w_{f3}..\ w_{fL})$
//construct four bit planes by reverse order of fragile water mark generating
Tamper location = compare (four bit planes, high 4 planes (S_a))
// compare four bit planes with the higher four bit planes of the image S_a
Replace (four bit planes, high 4 planes (S_a))
//Recovery by substituting four bit planes for the responding tampered pixels of S_a

RESULTS AND DISCUSSION

In this section, we present our experimental results in MATLAB and OMNet. 500 successive images with size 512×512 are tested to grouping, water mark generation, dual water mark embedding, authentication and image recovery in MATLAB. Water marked image transmission with packet loss is simulated in OMNet.

In the experiments, 128 bits robust water mark containing node ID and current timestamp and 512×512 bits fragile water mark is embedded.

Figure 3 shows three successive original images in the test image frames. Figure 4 shows three successive water marked images received in the sink with packet loss rate 5%. The robust water mark is embedded into Fig. 3a and the fragile water mark is embedded into image of Fig. 3b and then the robust water mark is embedded into Fig. 3b and the fragile water mark is embedded into image of Fig. 3c. Figure 5 shows the recovered images based on the test three image frames and the proposed scheme.

We use the Peak Signal to Noise Ratio (PSNR) coefficients to measure the quality of the water marked image, which is defined as follows:

$$\text{PSNR} = 10\log_{10}\left(\frac{(2^n-1)^2}{\text{MSE}}\right)$$

$$\text{MSE} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(X(i,j)-Y(i,j))^2$$

where, H and W denotes the height and width of the image, n denotes the bits of the pixel which generally be 8, X(i, j) and Y(i, j) denotes the pixel value of the original image and the water marked image.

The PSNR of the three water marked images in Fig. 4 are 42.37, 41.13 and 41.95, respectively, which means that the proposed scheme has good embedding performance.

The PSNR of the three recovered images in Fig. 5 are 40.87, 41.54 and 40.35, respectively, which means that the proposed scheme can effectively recover the lost parts of image with high quality.

Compared the recovered images in Fig. 5 with the original images in Fig. 3, the visual difference is insignificant. The results show the proposed scheme can recover the original images with good performance of invisibility.

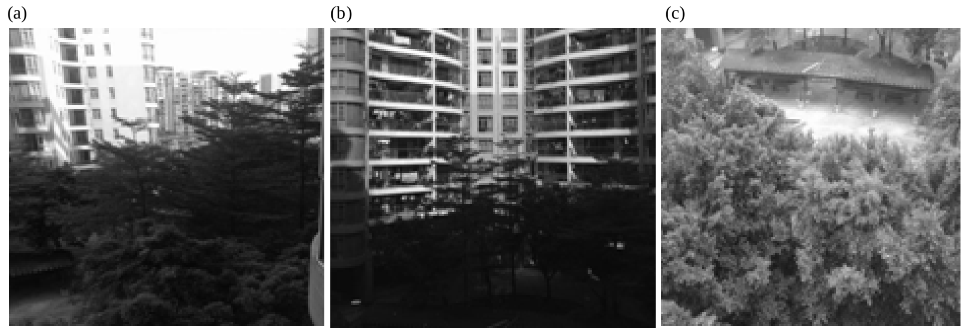

Fig. 3(a-c): Three successive original images, (a) Tree, (b) House and (c) Treetop

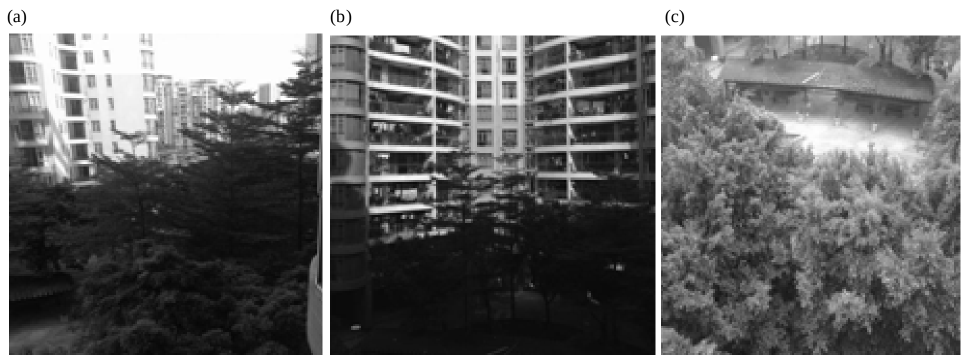

Fig. 4(a-c): Water marked images in sink, (a) Tree, (b) House and (c) Treetop

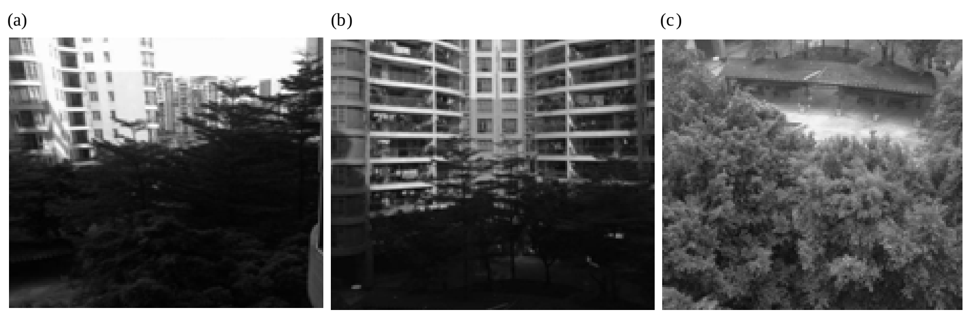

Fig. 5(a-c): Recovered images in sink, (a) Tree, (b) House and (c) Treetop

We use the Normalized Correlation (NC) (Hsu and Wu, 1998) coefficients to measure the similarity of original water marks and extracted water mark, which is defined as follows:

$$NC = \frac{\sum_{i=1}^{w}\sum_{j=1}^{m} w(i, j)w'(i, j)}{\sum_{i=1}^{w}\sum_{j=1}^{m}[w(i, j)]^2}$$

where, w' (i, j) denotes the extracted water mark and the w (i, j) denotes the referenced water mark. Table 1 shows the proposed scheme for robust water mark against different packet loss rates and Table 2 shows the proposed scheme for fragile water mark against different packet loss rates.

Table 1: Robust water mark against different packet loss rates

Image	10%	5%	3%
Figure 4a	PSNR = 39.03	PSNR = 42.37	PSNR = 43.36
	NC = 0.8269	NC = 0.8759	NC = 0.9469
Figure 4b	PSNR = 38.36	PSNR = 41.13	PSNR = 42.95
	NC = 0.8131	NC = 0.8578	NC = 0.9522
Figure 4c	PSNR = 38.96	PSNR = 41.95	PSNR = 43.89
	NC = 0.8211	NC = 0.8633	NC = 0.9591

In Fig. 6, we also compare the proposed scheme with the traditional FEC-based (Wu and Abouzeid, 2006) loss tolerance algorithm in MSNs using PSNR of the recovered image in sink under different packet loss rates. The results show that the proposed scheme has better capability of packet loss

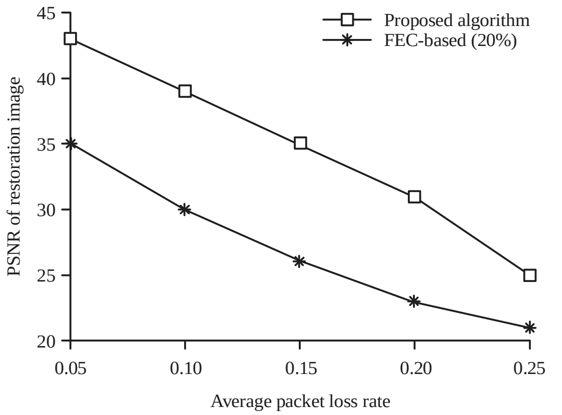

Fig. 6: Comparison of FEC-based and proposed algorithm

Table 2: Fragile water mark against different packet loss rates

Image	10%	5%	3%
Figure 5a	PSNR = 37.03	PSNR = 41.87	PSNR = 42.36
	NC = 0.6569	NC = 0.7459	NC = 0.7869
Figure 5b	PSNR = 36.36	PSNR = 42.54	PSNR = 43.95
	NC = 0.6131	NC = 0.6475	NC = 0.6822
Figure 5c	PSNR = 36.16	PSNR = 45.35	PSNR = 47.39
	NC = 0.6011	NC = 0.8033	NC = 0.8525

Table 3: Comparisons of water mark based schemes for MSNs

Schemes	Domain	Water marking No.	Function	Energy consumption
Wang (2013)	DWT	Single	Copyright	Low
Masood *et al.* (2010)	FFT	Single	Authentication	High
Kaur (2010)	DCT	Single	Authentication	High
Wang *et al.* (2008)	DWT	Single	Copyright	Low
Our propose	Spatial, DWT	Dual	Authentication and image recovery	High

tolerance than FEC-based algorithm. The reason is that FEC-based loss tolerance algorithm can only correct error packet of lossless data, while the proposed scheme embeds the water mark into another successive image and the embedded water mark can be used to recover the lost parts of image (Fig. 6).

We also compare the proposed scheme with several water mark based schemes for MSNs in Table 3. While otherschemes use only single water mark to achieve single function, the proposed scheme uses dual water mark in spatial and DWT domain to achieve dual function of authentication and image recovery. However, we found that two of the authors have used 'the two filter adaptive threshold' as an inserting technique (Wang, 2013; Wang *et al*., 2008) in DWT, while others have used the weight coefficient of the water mark in DCT (Kaur, 2010), the Orthogonal Frequency Davison Multiplexing (OFDM) in FFT (Masood *et al*., 2010), LSB and the weight coefficient of the water mark in DWT (Our proposed scheme), the adaptive threshold uses less power for MSN than the other techniques, because its positions are dynamically chosen to insert the water mark according to the network conditions, so that energy efficiency can be achieved.

CONCLUSION

In this study, a novel dual water marking based authentication and image recovery scheme for Multimedia Sensor Networks (MSNs) has been proposed. Different from other schemes, the proposed scheme verifies the identity and freshness of images and recovers original data completely by embedded dual water marks. Moreover, our water marking technique will not bring additional communication overhead. As a result, our technique can be used to recover the lost parts of images, which can thus efficiently improve the image quality with packet loss tolerance.

ACKNOWLEDGMENT

This study was supported by scientific and technological projects of Guangzhou (12C042011790), key program of NSFC-Guangdong union foundation (U1135002) scientific research project of Guangzhou municipal universities (2012A076), High-Level Talents Project of Institutions of Higher Education of Guangdong Province, projects of Guangzhou scholars (10A033D).

REFERENCES

Chen, M., V.C.M. Leung, S. Mao and Y. Yuan, 2007. Directional geographical routing for real-time video communications in wireless sensor networks. Comput. Commun., 30: 3368-3383.

Hemami, S.S. and T.H.Y. Meng, 1995. Transform coded image reconstruction exploiting interblock correlation. IEEE Trans. Image Process., 4: 1023-1027.

Hsu, C.T. and J.L. Wu, 1998. Multiresolution Water marking for digital images. IEEE Trans. Circuits Syst. II: Analog Digital Signal Process., 45: 1097-1101.

Kamel, I. and H. Juma, 2010. Simplified Water marking scheme for sensor networks. Int. J. Internet Port. Technol., 5: 101-111.

Kamel, I. and H. Juma, 2011. A lightweight data integrity scheme for sensor networks. Sensors, 11: 4118-4136.

Karlof, C., N. Sastry and D. Wagner, 2004. TinySec: A link layer security architecture for wireless sensor networks. Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, November 3-5, 2004, Baltimore, MD., USA., pp: 162-175.

Kaur, S., 2010. Digital Water marking of ECG data for secure wireless commuication. Proceedings of the International Conference on Recent Trends in Information, Telecommunication and Computing, March 12-13, 2010, Kochi, Kerala, pp: 140-144.

Masood, H., U. Sadiq-ur-Rehman and I. Khosa, 2010. Secure communication in WMSN. Proceedings of the International Conference on Information Networking and Automation (ICINA), October 18-19, 2010, Kunming, China, pp: 37-42.

Sun, H., J.W. Zdepski, W. Kwok and D. Raychaudhuri, 1997. Error concealment algorithms for robust decoding of MPEG compresse d video. Signal Process.: Image Commun., 10: 249-268.

Wang, H., D. Peng, W. Wang, H. Sharif and H.H. Chen, 2008. Energy-aware adaptive Water marking for real-time image delivery in wireless sensor networks. Proceedings of the IEEE International Conference on Communications, May 19-23, 2008, Beijing, China, pp: 1479-1483.

Wang, H.G., 2013. Communication-resource-aware adaptive Water marking for multimedia authentication in wireless multimedia sensor networks. Supercomput, 64: 883-897.

Wu, H. and A.A. Abouzeid, 2006. Error resilient image transport in wireless sensor networks. Comput. Networks, 50: 2873-2887.

Zhu, S., S. Setia and S. Jajodia, 2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Trans. Sen. Networks, 2: 500-528.