A ROI-BASED SELF-EMBEDDING METHOD WITH HIGH RECOVERY CAPABILITY

Hongliang Cai[1,2], *Huajian Liu*[2], *Martin Steinebach*[2], *Xiaojing Wang*[1]

[1] Chengdu Institute of Computer Applications, Chinese Academy of Sciences, China
[2] Fraunhofer SIT, Darmstadt, Germany

ABSTRACT

In this paper, a novel block-wise fragile image watermarking algorithm for tampering localization and recovery is proposed. The image is divided into Region of Interest (ROI) and Region of Non Interest (RONI). Considering the ROI-based self-embedding problem as a special erasure channel, fountain code is applied in our method to deal with the reference symbols loss. And to minimize quality degradation in ROI, the reference symbols for recovery are only embedded into RONI blocks. Theoretical analysis shows that the result is nearly optimal, and the experimental results demonstrate the proposed method can offer low payload and high tamper tolerance. And the quality of both the watermarked image and the reconstructed image is high.

Index Terms— watermarking, multimedia authentication, Region of Interest, fountain code

1. INTRODUCTION

The rapid development of information technology and wide availability of the image editing software makes acquisition and modification of digital images increasingly simple. So the integrity protection becomes a concerned topic in multimedia authentication applications. While digital watermarking is primarily used for copyright protection, various solutions have been proposed for image authentication [1].

Most of the existing watermarking schemes for image authentication are able to detect and localize the tamper. However, there are few schemes that have the ability to reconstruct the tampered content. In many applications, it is highly desired or even required to recover the tampered image regions.

In recent years, much research work has been done concerning watermarking with recovery ability [2-4]. Lee and Lin proposed a dual watermarking scheme in [2] to realize the reconstruction of tampered content. They maintain two copies of VQ indexing of each block so it will have another chance for the reconstruction when one copy is destroyed during the tampering. There are many other similar schemes which are known as self-embedding, where the reconstruction is achieved by keeping the reconstruction reference about itself using the replication strategy. This method, however, depends on high available embedding capacity and the recovery is restricted to the surviving rate of the replication.

An effective model for content reconstruction based self-embedding is proposed in [5], which regards the self-embedding problem as a special erasure channel and uses fountain code instead of copying method to eliminate the space waste and dependence on the mapping copies. It is the first method that can achieve high quality reconstruction under extensive tampering.

However, in [5] all the blocks are considered with equal importance. In some applications, such as medical images and the images as evidence in court, different regions of an image are of different importance. More protection and high quality are usually required for the important regions, which is defined as Region of Interest (ROI). The other regions, which is known as Region of Non-Interest (RONI), are of less importance. Ideally the quality of both watermarked and recovered ROI should be kept as high as possible. The RONI, which is usually the background, allows more quality loss and therefore more embedding strength or payload.

Some ROI-based watermarking schemes with recovery ability have been proposed in [6-14], the basic idea in most schemes is that, the copy of reference information of ROI is always embedded into RONI, and the authentication information is embedded into ROI itself. If ROI is tampered, the reconstruction is realized by extracting the copy from RONI. In [6, 8, 9] the reference recovery information about the whole ROI is embedded into RONI, in [7] the image is divided into small blocks, and the reference recovery information of each block in ROI is embedded into the mapping blocks in RONI. However, keeping a copy in the mapping blocks in RONI will suffer from the similar reference dependence problem mentioned in [5]. Tampering on the RONI blocks could result in recovery failure of some parts of the tampered ROI. Another drawback of this method is the reference waste. The copy of the whole ROI is kept when only part of ROI is tampered, the payload is not optimal, in fact the reference information should be indirectly proportional to the tamper rate from the point of information theory, the remaining ROI parts can be helpful in recovery. So we consider an improved method based on fountain code to show a new model for ROI and RONI.

In this paper we propose a novel ROI-based watermarking scheme to provide image integrity protection. The recovery reference information of ROI is embedded into RONI in block wise using erasure code. So the reference information of ROI can be spread over all the blocks of RONI and it can tolerate a high tampering rate in both ROI and RONI. The reference information of RONI can also be embedded into RONI if necessary. The optimal bound of the recovery capability is examined by analyzing the relationship between the embedding payload and the tamper rate. The performance of the proposed algorithm will be shown by the experiment results with tampering on grey images.

The rest of this paper is organized as follows. In Section 2, the proposed ROI-based self-embedding model for content reconstruction is introduced. The analysis is given in Section 3. Experimental results are presented in Section 4 and we conclude the paper in Section 5.

2. PROPOSED SCHEME

In this section we present our ROI-based self-embedding model and the watermarking scheme for the reconstruction.

2.1. ROI-based self-embedding model

Considering the tampering as message loss, the ROI based tamper and recovery problem can be regarded as this kind of special erasure channel:

(1) Consider the content of RONI as a communication channel. Note that not only the blocks in ROI but the blocks in RONI are also possibly tampered.

(2) Carrying the reference information part of ROI which is majority and perhaps also the reference information part of RONI which is minority;

(3) The blocks that fail in the authentication will be erased. The aim is to mainly recover the tampered blocks in ROI in good quality, while the tampered RONI blocks can be recovered as much as possible.

(4) The remaining authenticated blocks should contribute to the recovery of the tampered blocks.

To keep high fidelity, data embedded into ROI should be as few as possible. Hence, only the authentication bits of ROI blocks are embedded into ROI blocks, the recovery reference bits of ROI which is majority of the payload are embedded into RONI blocks. A part of reference information of RONI can also be embedded into RONI if recovery is required for RONI. The fountain code [15] which can generate potentially limitless encoding symbols from k original symbols and any slight more than k received encoding symbols can decode to recover the original symbols is applied in our method to get a nearly optimal payload for recovery. And in order to utilize the intact blocks in the recovery, Raptor code [16] which is one kind of fountain code should be systematic, which means the first k output encoding symbols are the same as k original symbols.

2.2. Proposed scheme

In this section the generation of reference bits for recovery, the reference data embedding and reconstruction process are introduced. And we focus on how to generate the payload as low as possible under a tamper rate. Similar to performance analysis under a given message loss rate in erasure channel in information theory, we will analyze the required embedding payload for the reconstruction under different tamper rates of ROI and RONI.

We assume that both ROI and RONI are divided into blocks of 8×8 pixels and there are N_1 blocks in ROI and N_2 blocks in RONI, t is the percentage of ROI blocks in all blocks, $t = N_1/(N_1 + N_2)$. Arbitrary E_1 blocks of ROI will be tampered, $E_1 = a \cdot N_1$, and arbitrary E_2 blocks of RONI are possibly destroyed, $E_2 = b \cdot N_2$. Two stage coding method will be applied to this kind of tampering.

The generation process for the authentication of ROI and payload part for ROI construction is described as below:

(1) Set the LSB of all ROI to 0, and calculate the 32 bits shorten hash value for each block of ROI, $H_{ROI} = \{H_1, \dots, H_{N1}\}$;

(2) Generate the representation symbols of all the ROI blocks into vector r_{ROI}, each block is presented in the same length, $g_b(.)$ can generate the bit stream of length b to represented the input image block;

$$r_{ROI} = r_1, \dots, r_{N1} = g_b(ROI_1), \dots, g_b(ROI_{N1})$$

(3)Encode $\{r_1, \dots, r_{N1}\}$ to generate $N_1(1 + a) + \epsilon$ encoded symbols α using the systematic Raptor Code. The former N_1 symbols which are the same as $\boldsymbol{r_{ROI}}$ are discarded, while remaining $E_1 + \epsilon$ symbols β_{ROI} will take part in the second encoding stage;

(4) Divide β_{ROI} into d segments $X = \{X_1, \dots, X_d\}$, $d = (1 - b) \cdot N_2 - \epsilon$, and encode X to generate N_2 output reference symbols for ROI using fountain code, $Y_{ROI} = \{Y_1, \dots, Y_{N2}\}$;

The generation process for the authentication of RONI and payload part for RONI construction is as below:

(1) Set 3 LSB of RONI blocks to 0, and generate the representation symbols of RONI blocks into vector j:

$$j_{RONI} = j_1, . , j_{N2} = g_b(RONI_1), . . , g_b(RONI_{N2})$$

(2) Encode $\{j_1, \dots, j_{N2}\}$ to generate $N_2(1 + b) + \epsilon$ encoded symbols α' using the systematic Raptor Code. The former N_2 symbols are also discarded, while the remaining $E_2 + \epsilon$ symbols β_{RONI} will take part in the second encoding stage;

(3) Divide β_{RONI} into d segments $X' = \{X_1', \dots, X_d'\}$, $d = (1 - b) \cdot N_2 - \epsilon$, and encode X' to generate N_2 output reference symbols for RONI using fountain code, $Z_{RONI} = \{Z_1, \dots, Z_{N2}\}$;

(4)Calculate the 32 bits shorten hash value h_i for Y_i , Z_i and the content of RONI block, $H_{RONI} = \{h_1, \dots, h_{N2}\}$.

In the embedding part, the hash value of each block of ROI is embedded into LSB bits itself. And in each RONI block the reference Y_i, Z_i and hash value h_i are embedded into the RONI block itself.

The authentication process:

Extract the hash value of each block and recalculate the hash value, if they are the same, the block is not tampered. If the block in RONI is authenticated, it means the embedded reference Y_i and Z_i are also available.

The reconstruction process:

The steps (1) to (3) are the reconstruction process for ROI:

(1) Decode from the remaining $(1-b)\cdot N_2$ available reference symbols Y_i' to get X.

(2) Rearrange X into $E_1+\epsilon$ pieces and joint with $(1-a)\cdot N_1$ regenerated representation symbols of the authenticated blocks in ROI, and decode to recover the representation symbols of the tampered blocks in ROI.

(3) Retrieve the tampered blocks in ROI using the function ${g_b}^{-1}(\cdot)$.

The steps (4) to (6) are the reconstruction process for RONI:

(4) Decode from the remaining $(1-b)\cdot N_2$ available reference symbols Z_i' to get X'.

(5) Rearrange X' into $E_2+\epsilon$ pieces and joint with $(1-b)\cdot N_2$ regenerate representation symbols of the authenticated blocks in RONI, and decode to recover the representation symbols of tampered blocks in RONI.

(6) Retrieve the tampered blocks using the function ${g_b}^{-1}(\cdot)$.

From the above we can see that the payload for recovery consists of 2 parts: one is Y_{ROI} and the other is Z_{RONI}. We can choose to generate only Y_{ROI} or both, which depending on if we need to recover RONI additionally.

3. ANALYSIS

First we analyze the success of recovery process. In the first decoding stage for ROI, the number of available Y_i' is $(1-b)\cdot N_2$, which is bigger than the number of original symbols d, and in the second decoding stage, there are $N_1+\epsilon$ symbols in total, so it is enough for decoding to recover the tampered blocks in ROI. For RONI, in the first decoding stage there are $(1-b)\cdot N_2$ available Z_i', it is bigger than d, and in the second decoding stage, there are $N_2+\epsilon$ symbols in total, it satisfies the decoding requirement, so the entire recovery must be successful.

In the following we focus on examining the relationship between the tamper rate and the payload for the reconstruction. The payload is evaluated by T which is the ratio of the size of reference data for reconstruction to the size of the original representation data. The tiny term ϵ/N will be disregarded in the result.

Let S_{ROI} and S_{RONI} denote the data size of the original representation information of ROI and RONI. The 2 payload parts are shown respectively. In ROI, the size of β_{ROI} in the first encoding stage is $D_{ROI1}=S_{ROI}\cdot\frac{E_1+\epsilon}{N_1}$. In the second encoding stage, β_{ROI} is rearranged into d pieces X and encoded into N_2 reference symbols Y_{ROI}. So the data size of Y_{ROI} and payload T_{ROI} are:

$$D_{ROI2}=D_{ROI1}\cdot\frac{N_2}{N_2-E_2-\epsilon}\approx S_{ROI}\cdot\frac{a}{1-b} \quad (1)$$

$$T_{ROI}=\frac{D_{ROI2}}{S_{ROI}}=\frac{a}{1-b} \quad (2)$$

For RONI, the data size in the first encoding stage is $D_{RONI1}=S_{RONI}\cdot\frac{E_2+\epsilon}{N_2}$. In the second encoding stage, the data size of Z_{RONI} and payload T_{RONI} is:

$$D_{RONI2}=D_{RONI1}\cdot\frac{N_2}{N_2-E_2-\epsilon}\approx S_{RONI}\cdot\frac{b}{1-b} \quad (3)$$

$$T_{RONI}=\frac{D_{RONI2}}{S_{RONI}}=\frac{b}{1-b} \quad (4)$$

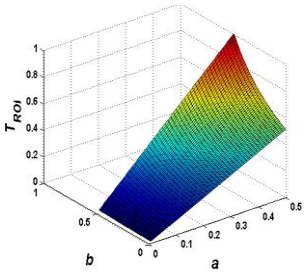

Fig. 1 Payload for ROI recovery

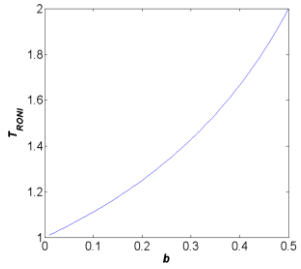

Fig. 2 Payload for RONI recovery

The evaluation about payload for ROI and RONI is shown in Fig. 1 and Fig. 2. And the overall payload for recovery of the image is

$$T=\frac{S_{ROI}\cdot T_{ROI}+S_{RONI}\cdot T_{RONI}}{S_{ROI}+S_{RONI}}=\frac{a\cdot S_{ROI}+b\cdot S_{RONI}}{(S_{ROI}+S_{RONI})\cdot(1-b)} \quad (5)$$

If we also consider another item of the representation bits size, assume that the length of the representation bits per block in ROI and RONI is l and q, there are $m\times m$ pixels in each block, we can get another evaluation about payload h by bpp (bit per pixel),

$$T=\frac{l\cdot t\cdot a+q\cdot(1-t)\cdot b}{[t\cdot l+(1-t)\cdot q]\cdot(1-b)} \quad (6)$$

$$h=\frac{l\cdot t\cdot a+q\cdot(1-t)\cdot b}{(1-t)(1-b)\cdot m^2} \quad (7)$$

From the results we can see that, the payload part T_{RONI} is actually the same as the upper bound in [5], and the other part T_{ROI} is also near optimal for the case of tampering in both ROI and RONI. Hence, the overall payload is a nearly optimal result. In order to achieve good quality in ROI, the ROI blocks should be represented by more bits, while the RONI blocks should be represented by fewer bits.

4. EXPERIMENTS

In our experiment the test images are 8-bit grey images. In each 8×8 ROI block the first 7 bit planes are transformed into DCT and divided into 15 groups, $S_i(x,y)$: $x,y\in\{0,\ldots,7\}$, $x+y=const$. The group 0 is quantized uniformly, the other groups are quantized with a Lloyd-Max code-book. The precision of the code-books is represented by a 15-D allocation vector: [8, 6, 4, 3, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]. At last we get $l=54$ representation bits for each ROI block. In the same way, in RONI the first 5 bits planes are participated in DCT transform and we use different allocation vectors to

get $q = 20$ representation bits. In each ROI block 32 shorten hash bits are embedded, and in each RONI block both the hash bits and the reference bits are embedded from the lowest LSB to 3th LSB as necessary.

To evaluate the proposed scheme, it is compared with the scheme in [7] which uses the classical copying strategy. For fair comparison, the same representation method and authentication method above are used in both schemes. The schemes are evaluated in different tampering scenarios.

In the first case, there is no tampering in RONI and the tamper rate a in ROI varies, set t=50%. As shown in Fig. 3 and Fig. 4, the payload for ROI recovery in our method is much lower than that in [7] and proportional to a, so the quality of watermarked image is significantly improved, while the quality of recovered image remains the same.

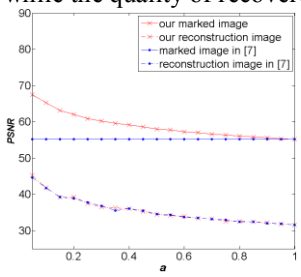

Fig 3. Image quality

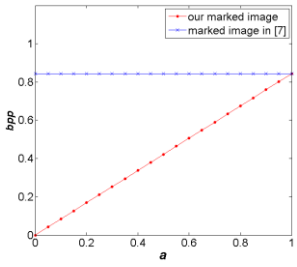

Fig. 4 Payload for ROI recovery

In the second case, we assume the tamper rate a about ROI is fixed while the tamper rate b about RONI varies, and only the recovery of tampered ROI is considered as many research before. Set t=50%, a=30%. The recovery performance is evaluated by P which is defined as the percentage of the tampered ROI blocks can be recovered.

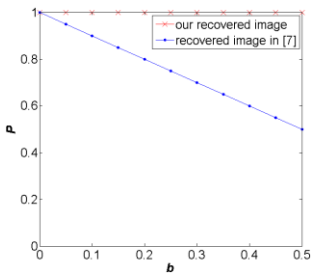

Fig. 5 Recovery performance

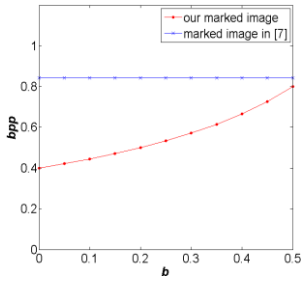

Fig. 6 Payload for ROI recovery

As shown in Fig. 5, when tampering occurs in both ROI and RONI, the scheme in [7] is not able to recover all the tampered blocks in ROI because a part of the reference information in RONI is destroyed. In contrast, the recovery of ROI in our scheme is always successful and complete. Moreover, as shown in Fig. 6, the payload in our scheme in this case is also lower than that in [7]. Because the payload is significantly decreased in our scheme, it enables our scheme to have the recover ability for the tampering out of ROI, which is not possible in the existing schemes.

So in the third case, we consider recovering the tampering in both ROI and RONI. The payload for recovering RONI is generated in a more compact way so that the tampered RONI could be reconstructed with lower quality.

Fig. 7 and Fig. 8 plot the payload in different tamper rates in ROI and RONI under different size of ROI.

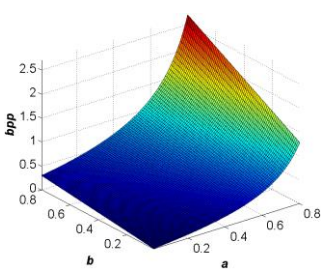

Fig. 7 t=30%

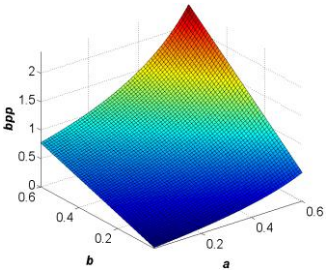

Fig. 8 t=60%

Fig. 7 and Fig. 8 shows that the payload is increasing gradually when a and b grow, and it is affect more by b. There is tradeoff between upper bound of tolerated tamper rate in ROI and tolerated tamper rate in ROI in the fixed payload. Supposed the 3 least significant bits in RONI are used for embedding, when t=30%, our scheme can recover up to 78% tampering in both ROI and RONI at the same time. If the tolerated tamper rate in ROI is set to 90%, the tolerated tamper rate in RONI will be 71%. When t=60%, the scheme can recover about 50% tampering in both ROI and RONI. When the tolerated tamper rate in ROI is set to 90%, the tolerated tamper rate in RONI will be 25%. And the expected PSNR of the watermarked image and the recovered image is higher than 37dB and 30dB respectively. In addition, the overall tamper rate can be higher than the bound 50% in [5] when the ROI part is not large.

If ROI needs to be recovered losslessly, the proposed scheme can be adapted by coding the LSB bits in ROI which are modified during embedding and storing them into RONI, and applying lossless representation function to ROI blocks.

5. CONCLUSION

We propose a novel ROI-based self-embedding model with high recovery ability. In order to introduce less interference to ROI, the authentication bits are embedded into ROI, and the reference information used for recovery is embedded into RONI. By considering the ROI-based self-embedding problem as a special erasure channel, the fountain code paradigm is adopted in the model to generate more effective results than the classical copying method. The theoretical analysis proves that the payload is nearly optimal, which results in high quality of watermarked image while the quality of the recovered image is not degraded. In addition, the propose scheme can also provide integrity protection and recovery for both ROI and RONI at the same time.

6. AKNOWLEDGMENTS

This work is supported by CASED (Center for Advanced Security Research Darmstadt).

7. REFERENCE

[1] Fridrich, Jessica. "Security of fragile authentication watermarks with localization." *Electronic Imaging 2002. International Society for Optics and Photonics*, 2002.

[2] Lee, Tien-You, and Shinfeng D. Lin. "Dual watermark for image tamper detection and recovery." *Pattern Recognition* 41.11 (2008): 3497-3506.

[3] Xinpeng Zhang and Shuozhong Wang. "Fragile watermarking with error-free restoration capability." *IEEE Transactions on Multimedia,* vol.10, no. 8, pp. 1490-1499, 2008.

[4] Zhenxing Qian, Guorui Feng, Xinpeng Zhang and Shuozhong Wang. "Image self-embedding with high-quality restoration capability." *Digital Signal Processing*, vol. 21, no. 2, pp. 278-286, 2011.

[5] Pawel Korus and Andrzej Dziech. "Efficient Method for Content Reconstruction with Self-Embedding." *IEEE Transactions on Image Processing*, vol. 22, no. 3, pp. 1134-1147, 2013.

[6] LEE, Hyung-Kyo, et al. "ROI medical image watermarking using DWT and bit-plane." *2005 Asia-Pacific Conference on . Communications*, pp. 512-515.

[7] Zain, J. M., & Fauzi, A. R. "Evaluation of medical image watermarking with tamper detection and recovery (AW-TDR). ", *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5661-5664, 2007.

[8] Memon, Nisar Ahmed, and S. A. M. Gilani. "NROI watermarking of medical images for content authentication." *12th IEEE International Multitopic Conference, 2008,* pp. 106-110, 2008.

[9] Badran, Ehab F., Maha A. Sharkas, and Omneya A. Attallah. "Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images." *National Radio Science Conference (NRSC)*, pp. 1-8, *2009.*

[10] Eswaraiah R, Reddy E S. "A Fragile ROI-Based Medical Image Watermarking Technique with Tamper Detection and Recovery", *2014 IEEE Fourth International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 896-899, 2014.

[11] Guo, Xiaotao, and Tian-ge Zhuang. "A region-based lossless watermarking scheme for enhancing security of medical data." *Journal of digital imaging*, vol. 22, no. 1, pp: 53-64, 2009.

[12] Lin, Shinfeng D., J. Lin, and C. Chen. " A ROI-based semi-fragile watermarking for image tamper detection and recovery." *International Journal of Innovative Computing, Information and Control*, vol.7, no. 12, pp. 6875-6888, 2011.

[13] Das, Sudeb, and Malay Kumar Kundu. "Effective management of medical information through ROI-lossless fragile image watermarking technique." *Computer methods and programs in biomedicine, vol.* 111, no. 3, pp. 662-675, 2013.

[14] Ren Juan, Wang Yun-Hong, Tan Tie-Niu, "A self-recovery algorithm based on region of interest," *ACTA AUTOMATICA SINICA*, vol. 30, no. 6, pp. 833-843, 2004.

[15] D.J.C. MacKay. "Fountain codes." *IEE Proceedings of Communications*, vol. 152, no. 6, IET, 2005.

[16] Amin Shokrollahi. "Raptor codes." *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2551-2567, 2006.