A NEW METHOD FOR IMAGE RECONSTRUCTION USING SELF-EMBEDDING

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

[1]Fraunhofer SIT, Darmstadt, Germany

[2]Chengdu Institute of Computer Applications, Chinese Academy of Sciences, China

ABSTRACT

In this paper we propose a new method for content reconstruction using self-embedding technology. As the content reconstruction problem can be regarded as a special kind of erasure channel, we use fountain code which has good performance in erasure channel to generate reference symbols for reconstruction. Theoretical analysis of success bound about maximal tamper rate is given and is verified by the Monte Carlo simulation. The experiments of a specific scheme show that our method can reduce the payload and improve the quality of the watermarked image, while still achieving high quality reconstruction and high tamper tolerance.

Index Terms— watermarking, content reconstruction, fountain code, self-embedding

1. INTRODUCTION

With the development of the information technology, multimedia can be modified easily with editing software. Hence, image authentication and recovery is becoming more and more important in multimedia security. In recent years, self-embedding [1] has been developed for image reconstruction in image authentication applications.

Reconstruction is usually achieved by embedding reconstruction reference symbols generated from the original content after the authentication process. The reconstruction reference part is generally the digital presentation of a quality reduced image, such as, the important DCT coefficients of each block [1-2], the halftone image [3], the average intensity of image block [4-5] or the VQ indexing of each block [6]. It is used to reconstruct the content of the tampered blocks when some regions are tampered.

Self-embedding schemes can be distinguished by three aspects, (1) the embedding payload and its impact on the watermarked image quality, (2) the maximal tampering rate which corresponds to the maximal region that can be reconstructed, and (3) the reconstruction fidelity. These factors are mutually competitive with each other. For instance, the scheme proposed in [8] is able to yield lossless reconstruction, while it can only tolerate 3.2% tampering. In [9] the authors introduced a scheme with high quality reconstruction which allows up to 35% tampering. The maximal tampering rate is increased to 59% in [10], but the quality of the reconstruction is rather low.

From different self-embedding strategies and their performances, we can extract two important challenges in self-embedding. First, in many self-embedding schemes the reference of a block is always embedded in a remote block. If both are destroyed by tampering, it will not be possible to recover the block any more. This problem is called reference dependence [11] or tampering coincident [12]. To solve the problem, one method is to maintain many copies in different blocks to improve the probability of successful reconstruction. In [6] and [13] two reference copies are inserted in mapping blocks. In [7] there are four copies of the index table via VQ for each block. The other method is to use redundancy sharing mechanism [9][12]. For example, the compressed features of each block were extended from 64 bits to 160 bits in [9]. The second challenge is called reference waste [11], which means that we do not need to recover all the reference pieces, but only the part which is tampered, so not all the embedded references contribute to the recovery.

Unlike the above-mentioned works which mainly focus on presenting a particular scheme and solve the problem partly, in [11] an effective method for content reconstruction with self-embedding is firstly proposed, it effectively solves the two challenges in self-embedding: reference dependence and reference waste. And it also provides the theoretical analysis of the maximal tamper rate by modeling the self-embedding to a revised erasure channel, which implies the inherent tradeoff between the max tamper rate and the payload. The results show that the method allows higher tampering rate than other self-embedding schemes with the same rate of reference information embedding per block. It is the first method that can maintain high quality reconstruction under extensive tampering. There are two main bounds of the max tampering rate. The upper bound can be achieved only when the reference blocks and reference symbols are aligned or when the erasure is continuous. In other common situation we can only rich up a typical bound which is lower. The main factor which decides whether the upper bound can be achieved is the misalignment between the reference blocks and symbols. Although the perfect alignment can be achieved by embedding multiple short symbols in a single block, it is not feasible due to high computation cost. Therefore, the proposed method in [11] can't always achieve the upper

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

bound. Nonetheless it introduced a general guideline for the construction of a self-embedding system.

Inspired by the idea that self-embedding can be regarded as a revised erasure channel, in this paper we propose a novel method for content reconstruction with self-embedding. We also use fountain code to encoding reference information because it spreads the reference information to the whole image which can effectively eliminate reference dependence. The regenerated reference bits of the authenticated blocks are also reused in the reconstruction stage which can contribute to the reference waste problem, but we use two stage coding method to generate the embedding symbols to avoid the misalignment problem. Both the theoretical analysis and the experimental results demonstrate that our method can always achieve the upper bound in [11] in any situation.

The rest of this paper is organized as follows. In Section 2, the proposed self-embedding model for content reconstruction is introduced. We analyze the reconstruction success bound in Section 3. Experimental results are presented in Section 4. Finally we conclude the paper in Section 5.

2. CONTENT RECONSTRUCTION METHOD

In this section we will first shortly introduce the self-embedding method by Korus and Dziech [11]. Then we discuss functions and notations of our approach.

2.1. Korus and Dziech's self-embedding method

There are three fundamental properties by which most authentication and reconstruction systems differentiate themselves from each other: the reference generation and reversed reconstruction method, the payload encoding method for reconstruction and the data embedding scheme. Except the payload encoding method, the other two parts can be presented in a general description.

Let I denote the original image which is divided into N pieces I_i, $i = 1, \dots, N$. Let $g_b(\cdot)$ denote a reference generation function for each block which produces b bits information. We will get a reference vector $\boldsymbol{r} = r_1, \dots, r_N = g_b(I_1), \dots, g_b(I_N)$. The inverse function ${g_b}^{-1}(\cdot)$ can be used to reconstruct the image block from the reference bit-stream.

The authentication part is usually realized by a hashing function $h(\cdot)$. The hash value is generated from the image block content I_i, the block payload Y_i, the block number i and a secret key k, $h_i = h(I_i, Y_i, i, k)$. The embedding process can be denoted by a function $f(I_i, Y_i, h_i) \to {I_i}'$, and the extraction function is ${f^{-1}}({I_i}') \to (Y_i, h_i)$.

The payload encoding method is different from others. Because the failure in the authentication after tampered can be regarded as an erasure in a revised erasure channel, the authors use random linear fountain code to encode from K reference symbols $X_i, i = 1,2, \dots, K$ which are rearranged from reference vector $\boldsymbol{r}$ to generate N embedding symbols $Y_i, i = 1,2, \dots, N$. So after the authentication process, some part of X_i which the i_{th} blocks are tampered are erased, we can decode to recover the part of Y_i which is interfered by the erasure of X_i, and the regenerated reference symbols of authenticated part are exploited in the decoding process.

Two main bounds are provided according to the formula between the block survival rate γ and the code rate λ. For the convenience to compare the theoretical result with our new method, we also give out the equivalent form between p which denotes the tamper rate and T which denotes the ratio of embedding reconstruction data size to original reference data size, in the method in [11], $p = 1 - \gamma, T = \frac{N}{K} = \frac{1}{\lambda}$.

The two main bounds are as below:

(1) The upper bound of max tampering rate

$$\gamma \geq \frac{\lambda}{\lambda+1} \tag{1}$$

Because $\gamma = 1 - p, \lambda = \frac{1}{T}$, we can get:

$$p \leq \frac{T}{T+1}. \tag{2}$$

(2) The typical bound of max tampering rate

$$\begin{cases} \gamma \geq \lambda\left(1 - \gamma^{\frac{1}{\lambda}}\right), & if\ \frac{1}{\lambda} \in N \\ \gamma \geq \lambda\left(1 - \gamma^{\frac{1}{\lambda}+1}\right), & otherwise \end{cases} \tag{3}$$

The equivalent form of (3) is as below:

$$\begin{cases} 1 - p \geq \frac{1}{\mathrm{T}}(1 - (1-p)^T), & if\ \ T \in N \\ 1 - p \geq \frac{1}{\mathrm{T}}(1 - (1-p)^{T+1}), & otherwise \end{cases} \tag{4}$$

The upper bound can be only achieved when the reference blocks and symbols are aligned or when the erasure pattern is continuous. Otherwise, the misalignment between the reference blocks and symbols will result in extra decoding demand for Y_i which will significantly degrade the performance.

2.2. Proposed Method

In this section we propose an improved image reconstruction method with self-embedding. We use a different reconstruction generating strategy which does not suffer from misalignment problem.

We also use the fountain paradigm in our method because it can spread the reference information over the whole image. Fountain code [14] is a new class of code which is designed and ideally suited for the erasure channel. Given a set of K source symbols it can generate potentially limitless encoding symbols according to bit-wise exclusive disjunction. The original information can be recovered if we receive slightly more than K encoding symbols. Raptor code [15] is a kind of fountain code, which can be systematic or non-systematic. In the systematic case, the symbols of the original part are included in the encoded symbols. In this paper we use systematic raptor code.

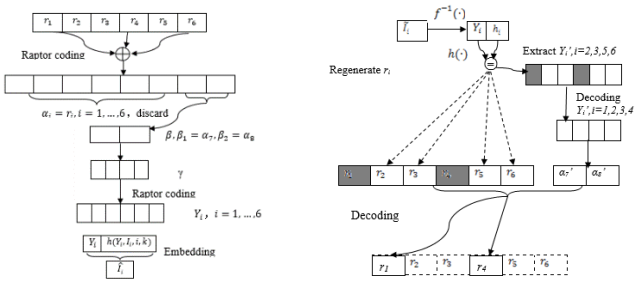

Fig. 2. (a) The reference encoding and embedding process (b) the reconstruction process after tampering

Let N denotes the total number of blocks, M denotes the number of authentic blocks, and E denotes the number of tampered blocks, $E = N - M$, the tamper rate is $p = E / N$.

The generation for the payload part for reconstruction is described as below:

(1) Divide the original image into N pieces and generate the reconstruction reference vector $\boldsymbol{r}$ from the significant part of the image, for example, MSB or high frequency of DCT.

$$\boldsymbol{r} = r_1, \dots, r_N = g_b(I_1), \dots, g_b(I_N)$$

(2) Encode $\boldsymbol{r}$ to generate $N + E + \epsilon$ encoded symbols α using the systematic Raptor Code. The former N symbols which are the same as $\boldsymbol{r}$ will be discarded, while the remaining $E + \epsilon$ symbols β will take part in the second encoding stage.

(3) In the second encoding stage, β are divided into $N - E - \epsilon$ pieces γ and encoded using Raptor code to produce N embedding symbols Y_i. Each symbol size is B bits.

The embedding process:

Calculate hash value of each block $h_i = h(I_i, Y_i, i, k)$, embed h_i and Y_i into the non-significant part which don't interfere with the reference generation, for example, LSB.

The authentication process:

Extract Y_i' and calculate the new hash value for the i^{th} block, $\widetilde{h_i} = h(I_i, Y_i', i, k)$ and compare it with h_i. If $\widetilde{h_i} = h_i$, $e_i = 1$ implies the block is authenticated, if $\widetilde{h_i} \neq h_i$, $e_i \neq 1$, the block is tampered. In this paper $N - E$ blocks are authenticated.

The reconstruction process:

(1) Extract the symbols Y_i' if the block is authenticated and regenerate the new reference block, $f^{-1}(I_i) \rightarrow Y_i'$, $g_b(I_i) \rightarrow r_i'$, when $e_i = 1$.

(2) Decode from the $N - E$ authenticated Y_i' to get the first $N - E - \epsilon$ symbols γ'.

(3) Rearrange γ' into $E + \epsilon$ pieces β'.

(4) Joint $N - E$ new reference symbols with $E + \epsilon$ pieces β' and decode the reference symbols of the tampered blocks.

(5) Recover the tampered blocks from the decoded reference symbols.

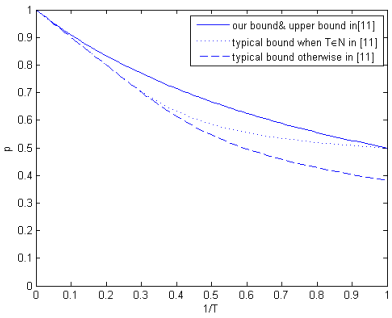

Fig. 3. Comparison of the success bounds

3. ANALYSIS

First we analyze the feasibility of the reconstruction process. As described in the last section, there will be two encoding stages and two decoding stages, in the first decoding stage, we need to decode $N - E - \epsilon$ symbols γ' from $N - E$ authenticated Y_i', it obviously satisfies the decoding condition. In the second decoding stage, after rearranging γ' into $E + \epsilon$ symbols β' and combining β' with the $N - E$ regenerate reference symbols, there will be $N + \epsilon$ symbols which is a little more than N, it is enough to decode to get E reference symbols of the tampered blocks.

Now we can draw out the successful reconstruction bound according to the relationship between T and p. As in fountain code the overhead $\epsilon / N \rightarrow 0$ when N is large, in the analysis process, the term ϵ / N will be disregarded as in [11]. And in the rearrangement process, the padding is also disregarded because it has little impaction on the result.

Let S denote the data size of the original reference information $\boldsymbol{r}$. After the first encoding stage, the data size of β is $D_1 = S \cdot \frac{E+\epsilon}{N}$. In the second stage, β is rearranged into $N - E - \epsilon$ pieces γ and encoded into N embedding symbols Y_i. So the data size of γ which is embedded is:

$$D_2 = D_1 \cdot \frac{N}{N-E-\epsilon} = S \cdot \frac{E+\epsilon}{N-E-\epsilon} = S \cdot \frac{p+\xi}{1-p-\xi} \quad (5)$$

Ignore the term ξ, we can get

$$T = \frac{D_2}{S} = \frac{p}{1-p} \quad (6)$$

$$p = \frac{T}{T+1} \quad (7)$$

We can see that our bound is the same as the upper bound in [11]. In our method it is a general result, no matter whether the tampering type is continuous or random. As shown in the Fig. 3, the solid line is our bound as well as the upper bound in [11], the dotted line which is lower is the typical bound in [11] because the reference blocks and symbols are not easy to align.

In order to validate the analytical reconstruction success bound, we perform tampering and reconstruction Monte Carlo simulations. In this experiment we set $T \geqslant 1$, $1 < hcf(b, B) < b$, the tamper rate p is random selected in (0, 1) and $p \cdot N$ tampered blocks are randomly selected. In each iteration, we perform encoding to get reconstruction

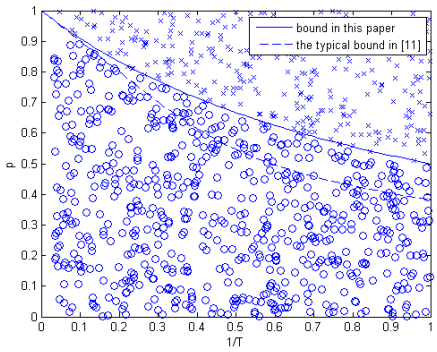

Fig. 4. Monte Carlo simulation about the success bound

reference information and embed, then we tamper the randomly selected p fractions, and reconstruct the new reference information. 1000 iterations are done, and if the reconstructed reference information of the tampered fraction is the same as the original reference information, the success is marked with circle, otherwise, the failure is marked with cross, as shown in Fig. 4.

4. EXPERIMENTAL RESULTS

In this section we provide test results for the proposed scheme under the model mentioned in section 2. The operations of our scheme follow the model, so we just describe the specific components.

For fair comparison, in our experiment we use the same reference generating method and hash value generating method as in [11]. The test image is divided into non-overlapping 8×8 blocks, and the 8 bit planes are divided into two parts. The last 3 LSB are used to embed reconstruction reference bits and hash at most, while the first 5 bit planes are regarded as important information and transformed into DCT to generate the reference bits. The DCT coefficients are divided into 15 groups, $S_i(x,y)$: $x, y \in \{0, \dots, 7\}$, $x + y = const$. The group 0 is quantized uniformly, and the other groups are quantized with a Lloyd-Max code-book [16]. The precision of the used code-books can be represented by a 15-D allocation vector: [8, 6, 4, 4, 4, 3, 3, 3, 2, 2, 0, 0, 0, 0, 0]. At last we will get $b = 157$ bits reference information.

Then we encode the reference information to get the embedding symbols which is regarded as the reconstruction part of payload. The size of this part is determined by p as (6). The 32 bits hash part are generated in the same way as in [11]. We will also use the same embedding strategy in both methods, the two parts are embedded from the lowest bit to 3 LSB on demand.

In this experiment we set $T<1$, as b is a prime, so in [11] $hcf(b, B) = 1$, This means that in [11] the reference blocks and the reference symbols are not aligned, it can't achieve the upper bound, but in our method we can.

We do experiments about the relationship between the tamper rate and the quality of embedded image and the

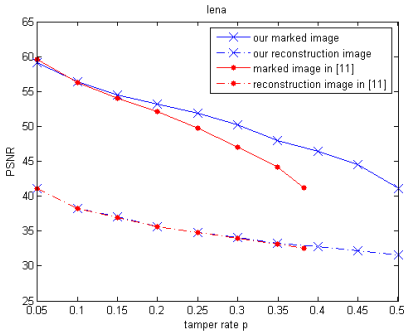

Fig. 5. Performance under different tamper rates

reconstruction image, the result is shown in Fig. 5. An example is shown in Fig. 6., when $p = 0.35$, $T = \frac{p+\xi}{1-p-\xi} \approx 0.56$ in our scheme, the bits for the reconstruction needed to embed in each block are $B = T \cdot b = 88$, while in [11] we can calculate $\lambda = 1.1863$, so $T = \frac{1}{\lambda} = 0.843$, $B = T \cdot b = 133$. From the two figures, we can see that if the tamper rate is the same, our scheme needs to embed less bits and can achieve better quality of embedded image. In other words, if we embed the same size of reconstruction reference bits, we can achieve higher tamper rate. At the same time, the quality of our reconstruction image is a bit better than in [11].

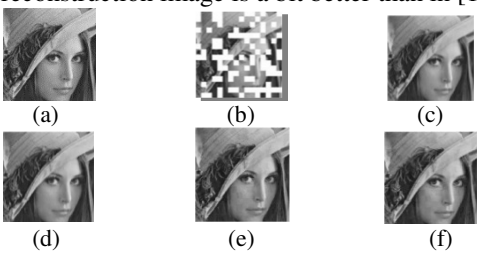

Fig. 6. The quality of the watermarked image and recovery image (a)original image (b)tampered image (c) the watermarked image in [11], PSNR = 44.12 dB (d) our watermarked image, PSNR = 47.98 dB (e) reconstruction image in [11], PSNR = 33.16dB (f)our reconstruction image, PSNR = 33.29dB.

5. CONCLUSION

In this paper we propose a new self-embedding method for content reconstruction which is suitable for different tamper patterns and various tamper rates. It avoids the misalignment problem in [11] and provides an improved method to deal with the two challenges in self embedding. The proposed method can always achieve the upper bound, no matter whether the tamper is continuous or random. Furthermore, the embedded payload is decreased in case of misalignment resulting in better image quality, while the quality of the recovered image is not degraded. The theoretical analysis and experimental results demonstrate that the proposed scheme outperforms the method in [11].

REFERENCES

[1] Jiri Fridrich, Miroslav Goljan. "Images with self-correcting capabilities," *Proceedings of International Conference on Image Processing (ICIP'99),* vol. 3. IEEE, 1999.

[2] Hong-Jie He, Jia-Shu Zhang and Fan Chen. "Adjacent-block based statistical detection method for self-embedding watermarking techniques." *Signal Processing*, vol. 89, no.8, pp. 1557-1566, 2009.

[3] Hao Luo, Shu-Chuan Chu and Zhe-Ming Lu. "Self embedding watermarking using halftoning technique." *Circuits, Systems & Signal Processing*, vol. 27, no.2, pp. 155-170, 2009.

[4] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt. "A secure and improved self-embedding algorithm to combat digital document forgery." *Signal Processing*, vol. 89, no. 12, pp. 2324-2332, 2009.

[5] Phen-Lan Lin, Chung-Kai Hsieh and Po-Whei Huang. "A hierarchical digital watermarking method for image tamper detection and recovery." *Pattern recognition*, vol. 38, no. 12, pp. 2519-2529, 2005.

[6] Tien-You Lee and Shinfeng D. Lin. "Dual watermark for image tamper detection and recovery." *Pattern Recognition*, vol. 41, no. 11, pp. 3497-3506, 2008.

[7] Chun-Wei Yang and Jau-Ji Shen. "Recover the tampered image based on VQ indexing." *Signal Processing*, vol. 90, no. 1, pp. 331-343, 2010.

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

[9] 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.

[10]Xinpeng Zhang, Shuozhong Wang and Guorui Feng. "Fragile watermarking scheme with extensive content restoration capability." *Digital Watermarking*. Springer Berlin Heidelberg, pp. 268-278, 2009.

[11] 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.

[12] Xinpeng Zhang, Shuoyhong Wang, Zhenxing Qian and Guorui Feng. "Reference sharing mechanism for watermark self-embedding," *IEEE Transactions on Image Processing*, vol. 20, no. 2, pp. 485-495, 2011.

[13] Chunlei Li, et al. "A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure." *Computers & Electrical Engineering*, vol. 37, no. 6, pp. 927-940, 2011.

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

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

[16] Stuart Lloyd. "Least squares quantization in PCM." *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 129-137, 1982.