Applied Mathematical Sciences, Vol. 11, 2017, no. 30, 1481 - 1494
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ams.2017.74134

An Efficient Reversible Watermarking Method and Its Application in Public Key Fragile Watermarking

Cao Thi Luyen and Pham Van At

Faculty of Information Technology
University of Transport and Communication
Ha Noi, Viet Nam

Abstract

In this paper a reversible watermarking method based on generalized integer transform of a vector with n pixels is presented. This method was firstly introduced by Alattar (called Alattar's method) has been concerned and expanded because it can achieve high embedding capacity without losing the implication of the cover. According to Alattar's method, n-1 bits could be embedded into a vector with n pixels if this vector is expandable. The evaluation of vector expandability has exponential complexity in the length of the vector, so computing time is inversely proportional complexity of the embedding capacity. This is why this method can only use the vector with 3 or 4 pixels in practical. The larger the vector size is, the higher the embedding capacity is, thus, the embedding ability is not gained as mentioned in theoretical analysis. This paper proposes the expandable and changeable criteria for a vector with linear complexity in the length of a vector. Therefore, the embedding capacity of Alattar's method is really obtained as theory indicated. Experimental results show that schemes which use the proposed algorithms to check if a vector is expandable and changeable, are much faster and outperform several widely different (used) schemes in terms of computational complexity. The public key watermarking based on the proposed reversible algorithm is faster and more efficient as well as detecting any modifications of the watermarked image.

Keywords: reversible watermarking, difference expansion, integer transform, prediction error expansion, public key

1 Introduction

Digital watermarking is a technique to embed useful data (watermark) into media such as image, audio, video etc... The embedded watermark can be detected or extracted out in order to reveal the real owner/identity of the digital media. There are many ways to classify watermarking. For using objectives, watermarking techniques are classified into robust, semi-fragile and fragile watermarking. Robust watermarking is applied in copyright protection purposes while fragile watermarking is to detect any pixel changes and to locate changed parts of the image [1]. Watermarking method is divided into private key and public key watermarking regard to key. This paper relates to public key fragile reversible watermarking. Reversible watermarking is a method such that restoring host image and extracting original watermark are necessary.

Many valuable reversible watermarking methods have been researched in the literature. Some primary approaches are proposed such as difference expansion (DE), based compression, histogram shifting (HS) and prediction error expansion (PEE). The most currently interested technique is based on difference expansion. The first DE proposed by Tian [5] is an effective approach. DE technique is carried out on pairs of pixels, and each expandable pair is embedded by one bit. This method can obtain a high capacity with a low distortion. Tian's method is a fundamental work of reversible watermarking and has recently been researched and expanded [2, 4, 6, 7, 9, 10, 17]. For instance, Alattar [3] generalizes the DE technique by taking a set of n pixels rather than a pair of pixels [8, 11, 12, 13, 14 and 15] which achieves a significant improvement incorporating the DE technique with other methods such as histogram shifting, prediction error expansion (PEE), etc…, in order to gain higher capacity and a lower distortion.

In this paper, we focus on Alattar's method since this technique can achieve a high embedding ability and good imperceptibility. According to Alattar, n-1 subtractions $u_i - u_1, i = 2,3 \ldots n$ are formed by a vector with n pixels $(u_1, u2, \ldots, u_n)$, where one bit is embedded in each subtraction and u_1 is called the base element. [6] improved Alattar's scheme by changing the base element into the middle element ($u_{n/2}$) of the vector to create smaller subtractions. As a result, watermarked image quality is better. [4] selected an element that has value closed to the mean of the vector as base element and the embedding technique guarantees restoring of that base element. [7] chose the base element as [6] but embedded as Lee's work. Weng et al. [16] applied Alattar's method with n-1 pixels $(u_1, u2, \ldots, u_{n-1})$ to create n-2 subtractions $u_i - u_{i-1}, i = 2,3 \ldots n-1$ based on two neighbouring elements to embed n-2 bits. The last subtraction was established by PEE method to hide 1 bit in itself. The larger size of the vector is, the higher capacity is. The vector should be checked if it is expandable and changeable before embedding data. However, [4] or [7] did not consider those conditions so they did not evaluate exactly the embedding ability. Alattar and Weng based methods had troubles of overflow or underflow, especially for large size vector due to the performance of a large number of operations. These methods only executed the vector with 3 or 4 pixels in practice because of exponential computing

complexity in terms of the length of the vector. Computing time is inversely proportional complexity of the embedding capacity. For larger vectors, take a vector in size of 16 pixels as an example, it is divided into 4 sub-vectors in size of 4 pixels. Then 3 bits could be embedded in each sub-vector. Therefore, only 12 bits were embedded into a vector with 16 pixels. This means that the embedding ability is not gained as theoretical analysis introduced. This paper proposes the simple valuation criterion for Alattar or Weng based methods, thereby it reduces the computational complexity while increases the embedding ability. Consequently, the capacity of Alattar or Weng based methods is much better.
The rest of the paper is organized as follows: In section 2, the related works such as Tian'method, Alattar and Weng's technique are described. The proposed expandable and changeable criteria are presented and proved in section 3. In section 4, the public key fragile watermarking scheme using the proposed algorithm is presented. The conclusion is revealed in section 5.

2 Related word

2.1 Tian's method

Tian proposed the reversible method for a pair of pixels, the details of the method are presented in the Table 1.

Table 1. The Embedding and the extracting procedures of Tian's method

The embedding procedure Input: pixels x and y, b is secret bit Output: x' and y'	**The extracting procedure** Input: x' and y' Output: x, y and b
Step 1: Calculate the h and l: $h = x - y, \quad l = \left\lfloor \frac{x+y}{2} \right\rfloor$ **Step 2:** Expand h: $h' = 2h + b$ **Step 3:** Compute : $x' = l + \left\lfloor \frac{h'+1}{2} \right\rfloor, \quad y' = l - \left\lfloor \frac{h'}{2} \right\rfloor$	**Step 1:** h' and l is determined: $h' = x' - y', \; l = \left\lfloor \frac{x'+y'}{2} \right\rfloor$ **Step 2:** Recover vectors *B* and *V*: $b = h' \bmod 2$ **Step 3:** Extract x and y: $h = \left\lfloor \frac{h'}{2} \right\rfloor$, $x = l + \left\lfloor \frac{h+1}{2} \right\rfloor, \; y = l - \left\lfloor \frac{h}{2} \right\rfloor$

2.2 Alattar and Weng's methods

In this section, Alattar and Weng's methods are described. Firstly, the notations are fixed as the followings: Consider a positive integer n. A host grayscale image is divided into non-overlapped blocks of n pixels denoted by $U = (u_1, u_2, \ldots, u_n) \in Z^n$ .The secret message $B = (b_2, ..., b_n) \in Z_2^{n-1}$ is embedded into vector *U*. Assume that the corresponding watermarked block is $U' = \left(u_1^{'}, .., u_n^{'}\right) \in Z^n$.

Next, the detail of those embedding and restoring methods based on generalized integer transform are presented in the Tables 2 and Table 3.

Table 2. The Embedding and the recovering procedures of Alattar's method

The embedding procedure	**The recovering procedure**
Input: Vector U of n pixels and secret bits B $U=(u_1,u_2,\ldots,u_n)\in Z^n,\ B=(b_2,...,b_n)\in Z_2^{n-1}$ Output: $U'=(u_1^{'},..,u_n^{'})\in Z^n$	Input: $U'=(u_1^{'},..,u_n^{'})\in Z^n$ Output: $U=(u_1,u_2,\ldots,u_n)\in Z^n,\ B=(b_2,...,b_n)\in Z_2^{n-1}$
Step 1: Calculate the vector $V=(v_1,v_2,..,v_n)\in Z^n$: $v_1=\overline{u_n}=\left\lfloor\frac{\sum_{i=1}^{n}u_i}{n}\right\rfloor$ (1) $v_j=u_j-u_1, j=2..n$ (2) **Step 2:** $V'\in Z^n$ is given by equation: $v_1^{'}=v_1; v_j^{'}=2v_j+b_j,\ \ j=2..n$ (3) **Step 3:** Compute $U'=(u_1^{'},..,u_n^{'})\in Z^n$: $u_1^{'}=v_1-\left\lfloor\frac{\sum_{i=2}^{n}v_i^{'}}{n}\right\rfloor$ (4) $u_j^{'}=v_j^{'}+u_1^{'}, j=2..n$ (5)	**Step 1:** $V=(v_1^{'},..,v_n^{'})\in Z^n$ is determined: $v_1^{'}=\overline{u^{'}_n}=\left\lfloor\frac{\sum_{i=1}^{n}u^{'}_i}{n}\right\rfloor$, $v_j^{'}=u^{'}_j-u_1^{'}, j=2..n$ **Step 2:** Recover the vectors *B* and *V*: $b_j=v_j^{'} \bmod 2, v_1=v_1^{'},\ v_j=\left\lfloor\frac{v_j^{'}}{2}\right\rfloor,\ \ j=2..n$ (6) **Step 3:** Extract the vector $U=(u_1,u_2,\ldots,u_n)\in Z^n$: $u_1=v_1^{'}-\left\lfloor\frac{\sum_{i=2}^{n}v_i}{n}\right\rfloor, u_j=v_j+u_1,\ j=2..n$

Table 3. The Embedding and the recovering procedures Weng's method

The embedding procedure	**The recovering procedure**
Input: Vector U of n pixels and secret bits B $U=(u_1,u_2,\ldots,u_n)\in Z^n,\ B=(b_2,...,b_n)\in Z_2^{n-1}$ Output: $U'=(u_1^{'},..,u_n^{'})\in Z^n$	Input: $U'=(u_1^{'},..,u_n^{'})\in Z^n$ Output: $U=(u_1,u_2,\ldots,u_n)\in Z^n,\ B=(b_2,...,b_n)\in Z_2^{n-1}$
Step 1: Vector $V=(v_1,v_2,..,v_n)\in Z^n$ is calculated: $v_1=\overline{u_n}=\left\lfloor\frac{\sum_{i=1}^{n-1}u_i}{n}\right\rfloor$ (7) $v_j=u_j-u_{j-1}, j=2..n-1$ (8) $v_n=u_n-v_1$ (9) **Step 2:** $V=(v_1^{'},..,v_n^{'})\in Z^n$ is obtained by applying the formula (3). **Step 3:** Compute the vector $U'=(u_1^{'},..,u_n^{'})\in Z^n$: $u_1^{'}=v_1^{'}-\left\lfloor\frac{(n-2)v_2^{'}+(n-3)v_2^{'}+\ldots+v_{n-1}^{'}}{n-1}\right\rfloor$ (10) $u_i^{'}=v_i^{'}+u_{i-1}^{'}, j=2\cdots n-1$ (11) $u_n^{'}=v_n^{'}+v_1^{'}$ (12)	**Step 1:** Determine the vector $V=(v_1^{'},..,v_n^{'})\in Z^n$ as the following equations: $v_1^{'}=\overline{u^{'}_n}=\left\lfloor\frac{\sum_{i=1}^{n-1}u^{'}_i}{n-1}\right\rfloor$ $v_j^{'}=u_j^{'}-u_{j-1}^{'}, j=2..n-1$ $v_n^{'}=u_n^{'}-v_1^{'}$ **Step 2:** Recover the vectors *B* and *V* by applying the formulas (6). **Step 3:** Extract the vector $U=(u_1,u_2,\ldots,u_n)\in Z^n$: $u_1=v_1^{'}-\left\lfloor\frac{\sum_{i=2}^{n-1}(n-i)v_i}{n-1}\right\rfloor$ $u_j=v_j+u_{i-1}, j=2..n-1$ $u_n=v_n+v_1$

2.3 Expandable and changeable definitions

Definition 1:

Vector $U=(u_1,u_2,\ldots,u_n)\in Z^n$ is expandable if all u_i' of U' in embedding procedure satisfy $0 \le u_i' \le 255, i = 1..n$.

Definition 2:

$U=(u_1,u_2,\ldots,u_n)\in Z^n$ is changeable if all u_i' of U' in embedding procedure falls in the range of $[0,255], i = 1..n$ where the transforming V into V' via equation (13) instead of formula (3):

$$v_1' = v_1;\ v_j' = 2\left\lfloor \frac{v_j}{2} \right\rfloor + b_j,\ \ j = 2..n \tag{13}$$

Therefore, *B* and *V* are recovered in extracting stage by the below equation instead of formula (6):

$$b_j = v_j' \bmod 2, v_j = 2\left\lfloor \frac{v_j'}{2} \right\rfloor + b_j,\ \ j = 2..n$$

2.4 Comments

The secret data *B* is embedded into *U* if all elements of U' are in $[0,255]$, therefore, it's necessary to check the expandable or changeable condition of *U*. To check the expandable or changeable condition of vector U of n pixels, it's necessary to test 2^{n-1} difference vectors U' in $[0,255]$ corresponding to 2^{n-1} difference watermarks *B* of n-1 bits. We have to implement n multiplications/divisions (excluding the addition or subtraction) to determine U' of n pixels. $2 \times n$ comparing operations are performed to check if each $U'$is in $[0,255]$ or not.

Thus, $2^{n-1} \times n$ multiplications - divisions and $2^n \times n$ comparison operators should be done to examine a vector of n pixels if it is expandable or changeable.

For example, if the host image of 512×512 is divided into sub-sequences (vector) with length n = 16, the number of sequence *U* is 32768. Then, to determine whether a sub-sequence is expandable/changeable or not we need to do:

$$2^{15} \times 16 \times 32768 = 1719869184$$

(Multiplications/Divisions)

$$2^{16} \times 16 \times 32768 = 34359738368$$

(Comparison operators)

In fact, [3, 16] and Alattar or Weng's based methods [4, 6 and 7] are only experimental for vectors with 3 or 4 pixels. The larger vector size is not feasible because of the huge computational complexity, but the larger it is, the higher capacity is. Indeed, to be able to experiment on a 16-element vector, Alattar separated the vector into four sub-vectors in size of 4. Each sub-vector embeds 3 bits, so there are only 12 bits embedded in the 16-element vector, instead of 15 bits as mentioned theory. We propose algorithms to test the expandability and chan-

geability of a vector with linear complexity in the length of the vector, the algorithms lead to significantly reduced computation time. Therefore, a larger size vector is done, and the high embedding possibility of schemes in [3, 16] as well as the related schemes [4, 6 and 7] is actually obtained in practical

3 The algorithms

3.1 For Alattar based method

Theorem 1: For a greyscale image – valued vector $U=(u_1,u_2,\ldots,u_n)$ we say U is expandable if and only if:

$$n(v_1-255)\le S_{AE}<n(v_1+1)-(n-1) \tag{14}$$

$$n-1+n(v_1+2v_i-255)\le S_{AE}<n(v_1+2v_i+1)-(n-2) \tag{15}$$

$$i=2,3,\ldots,n$$

Where $S_{AE}=2\sum_{i=2}^{n}v_i$

Proofs: From (2) to (5) formulas, we have:

$$u_1^{'}=v_1-\left\lfloor\frac{S_{AE}+\sum_{i=2}^{n}b_i}{n}\right\rfloor \tag{16}$$

$$u_i^{'}=v_1+2v_i-\left\lfloor\frac{S_{AE}+\sum_{j=2,j\neq i}^{n}b_i-(n-1)b_i}{n}\right\rfloor \tag{17}$$

For simplicity, $Max\{u_1'|B=(b_2,\cdots,b_n)\epsilon Z_2^{n-1}\}$, $Min\{u_1'|B=(b_2,\cdots,b_n)\epsilon Z_2^{n-1}\}$, $Max\{u_i'|B=(b_2,\cdots,b_n)\epsilon Z_2^{n-1}\}$ and $Min\{u_i'|B=(b_2,\cdots,b_n)\epsilon Z_2^{n-1}\}$ are denoted by $Maxu_1', Minu_1', Maxu_i'$ and $Minu_i'$ respectively.

From (4), (4), (16) and (17), we conclude:

$$Maxu_1^{'}=v_1-\left\lfloor\frac{S_{AE}}{n}\right\rfloor \tag{18}$$

$$Minu_1^{'}=v_1-\left\lfloor\frac{S_{AE}}{n}+\frac{n-1}{n}\right\rfloor \tag{19}$$

$$Maxu_i^{'}=v_1+2v_i-\left\lfloor\frac{S_{AE}}{n}-\frac{n-1}{n}\right\rfloor \tag{20}$$

$$Minu_i^{'}=v_1+2v_i-\left\lfloor\frac{S_{AE}}{n}+\frac{n-2}{n}\right\rfloor \tag{21}$$

Suppose that U is expandable by definition 1, then $Maxu_i^{'}\le 255$ and $Minu_i^{'}\ge 0, i=1,..,n$.

From (18) to (21) equations we get (14) and (15).
Thus, the necessary condition is proven.
In contrast, if formulas (14) and (15) are satisfied then from (18), (19), (20) and (21) we infer that:
$Max u_i^{'} \le 255$ and $Min u_i^{'} \ge 0, i = 1,..,n$.

It derives that U is expandable by definition 1. Therefore, the sufficient condition is proven.

In conclusion, theorem 1 is proven.
Theorem 2: For a greyscale image – valued vector $U = (u_1, u_2, \ldots, u_n)$, we say U is changeable if and only if:

$$n(v_1 - 255) \le S_{AC} < n(v_1 + 1) - (n-1) \quad (22)$$

$$n - 1 + n(v_1 + 2\left\lfloor \frac{v_i}{2} \right\rfloor - 255) \le S_{AC} < n(v_1 + 2\left\lfloor \frac{v_i}{2} \right\rfloor + 1) - (n-2) \quad (23)$$

$$i = 2,3,\ldots,n$$

Where $S_{AC} = 2\sum_{i=2}^{n} \left\lfloor \frac{v_i}{2} \right\rfloor, i = 2,3..,n$

Proofs:
It derives that U is changeable by definition 2. Thus, the sufficient condition is proven. In conclusion, theorem 2 is easily obtained from theorem 1: just replace v_i with $\left\lfloor \frac{v_i}{2} \right\rfloor$.

3.2 For Weng's based method

Theorem 3: For a greyscale image – valued vector $U = (u_1, u_2, \ldots, u_n)$, we say U is expandable if and only if:

$$v_1 - 255 \le T < v_1 - \frac{n}{2} \quad (24)$$

$$v_1 + 2\sum_{j=2}^{k} v_j - 255 - \frac{(n-k-1)(n-k)}{2(n-1)} \le 2T < v_1 + 2\sum_{j=2}^{k} v_j + 1 + \frac{k(k-1)}{2(n-1)},$$
$$k = 2 \ldots n-1 \quad (25)$$

$$0 \le 2v_n + v_1 \le 254 \quad (26)$$

Where $T = \frac{2\sum_{i=2}^{n-1}(n-i)v_i}{n-1}$

Proofs:
From (3), (10), (12), (13), (14) and (15) formulas we get:

$$u_1' = v_1' - \left\lfloor \frac{(n-2)v_2' + (n-3)v_2' + \cdots + v_{n-1}'}{n-1} \right\rfloor$$
$$= v_1$$
$$- \left\lfloor \frac{2(n-2)v_2 + 2(n-3)v_3 + \cdots + 2v_{n-1} + (n-2)b_2 + (n-3)b_3 + \cdots + b_{n-1}}{n-1} \right\rfloor$$
$$= v_1 - \left\lfloor \frac{2\sum_{i=2}^{n-1}(n-i)v_i + \sum_{i=2}^{n-1}(n-i)b_i}{n-1} \right\rfloor \quad (27)$$

$$u_k' = v_1 + 2\sum_{j=2}^{k} v_j$$
$$- \left\lfloor T + \frac{-b_2 - 2b_3 - \cdots (k-1)b_k + (n-k-1)b_{k+1} + \cdots + b_{n-1}}{n-1} \right\rfloor$$

$$k = 2 \ldots n-1 \quad (28)$$

$$u_n' = 2v_n + b_n + v_1 \quad (29)$$

We find that:

$$Max\, u_1' = v_1 - \lfloor T \rfloor \quad (30)$$

$$Min\, u_1' = 2v_1 - \left\lfloor T + \frac{n-2}{2} \right\rfloor \quad (31)$$

$$Max\, u_k' = v_1 + 2\sum_{j=2}^{k} v_j - \left\lfloor T - \frac{k(k-1)}{2(n-1)} \right\rfloor,$$

$$Min\, u_k' = v_1 + 2\sum_{j=2}^{k} v_j - \left\lfloor T + \frac{(n-k-1)(n-k)}{2(n-1)} \right\rfloor, k = 2 \ldots n-1 \quad (32)$$

$$Max\, u_n' = 2u_n - \overline{u_{n-1}} + 1 \quad (33)$$

$$Min\, u_n' = 2u_n - \overline{u_{n-1}} \quad (34)$$

Assumes that U is expandable by definition 1, then $Max u_i' \le 255$ and $Min u_i' \ge 0, i = 1,..,n$

From (30) to (34) formulas we get (24), (25) and (26).
So, the necessary condition is proven.
In contrast, if formulas (24), (25) and (26) are satisfied then from (30) to (34) formulas we infer that:
$Max u_i' \le 255$ and $Min u_i' \ge 0, i = 1,..,n$.
It derives that U is expandable by definition 1. Thus, the sufficient condition is proven.

In conclusion, theorem 3 is proven.

Theorem 4
For a greyscale image – valued vector $U = (u_1, u_2, \ldots, u_n)$, we say U is changeable if and only if:

$$v_1 - 255 \le Q < v_1 - \frac{n}{2}$$

$$v_1 + 2\sum_{j=2}^{k}\left\lfloor\frac{v_j}{2}\right\rfloor - 255 - \frac{(n-k-1)(n-k)}{2(n-1)} \le Q < v_1 + 2\sum_{j=2}^{k}\left\lfloor\frac{v_j}{2}\right\rfloor - 1 + \frac{k(k-1)}{2(n-1)}, k = 2 \ldots n-1$$

$$0 \le 2\left\lfloor\frac{v_n}{2}\right\rfloor + v_1 \le 254$$

Where: $Q = \frac{2\sum_{i=2}^{n-1}(n-i)\left\lfloor\frac{v_i}{2}\right\rfloor}{n-1}$

Proofs
Theorem 4 is easily proven from theorem 3 by replacing v_i with $\left\lfloor\frac{v_i}{2}\right\rfloor$.

3.3 Experiment results

We use the images of 256x256 as demonstrated in Fig.1 to evaluate the complexity of our proposed methods, compared with that of the related schemes. The experimental results are shown in Tables 4 through 9. From the tables, we can see that the smaller value in each table entry reveals the low scheme's complexity.


Lena


Airplane


Pepper

Fig. 1. Host Images

Table 4. Complexity of Alattar's method for Lena

Vector size	Alattar's method		Improved Alattar's method	
	Expandable	Changeable	Expandable	Changeable
4	11.2856	11.6785	1.81652	1.98
9	142.1508	150.3140	0.9538	0.9194
16	N/A	N/A	0.5647	0.5113

Table 5. Complexity of Alattar's method for Airplane

Vector size	Alattar's method		Improved Alattar's method	
	Expandable	Changeable	Expandable	Changeable
4	10.7947	15.2970	1.7221	2.0622
9	132.8403	184.6235	0.8272	1.0993
16	N/A	N/A	0.5506	0.6906

Table 6. Complexity of Alattar's method for Pepper

Vector size	Alattar's method		Improved Alattar's method	
	Expandable	Changeable	Expandable	Changeable
4	11.4777	12.0461	1.8658	1.9657
9	157.2067	150.4259	0.906988	0.9684
16	N/A	N/A	0.582164	0.5684

Table 7. Complexity of Weng's method for Lena

Vector size	Weng et al's method		Improved Weng et al's method	
	Expandable	Changeable	Expandable	Changeable
4	11.2568	10.8362	1.9669	2.2394
9	135.6471	138.6591	0.91460	1.0464
16	N/A	N/A	0.6361	0.6535

Table 8. Complexity of Weng's method forAirplane

Vector size	Weng et al's method		Improved Weng et al's method	
	Expandable	Changeable	Expandable	Changeable
4	11.7181	12.0886	6.5977	2.6178
9	141.4106	160.1235	2.5938	1.1787
16	N/A	N/A	0.7374	0.7080

Table 9. Complexity of Weng's method for Pepper

Vector size	Weng et al's method		Improved Weng et al's method	
	Expandable	Changeable	Expandable	Changeable
4	11.8727	12.5161	1.9214	2.1564
9	156.4367	160.4357	0.9198	0.9592
16	N/A	N/A	0.5871	0.5912

Tables 4 through 9 show that the time consuming of the proposed methods is much lower than the related works. This means that applying the proposed methods in reversible data hiding or watermarking schemes can reduce the computing complexity of Alattar and Weng based methods. On the other hand, proposed evaluations if block changeable are simple, so the high embedding capacity of the Alattar and Weng methods actually achieve theoretical analysis.

4 The public key fragile watermarking scheme

We use the SHA1 as our hash function and the RSA public key encryption algorithm for encoding and decoding.

4.1 Watermark Embedding

The watermark embedding procedures of the proposed public key fragile scheme for authentication problem is shown in Fig. 2.

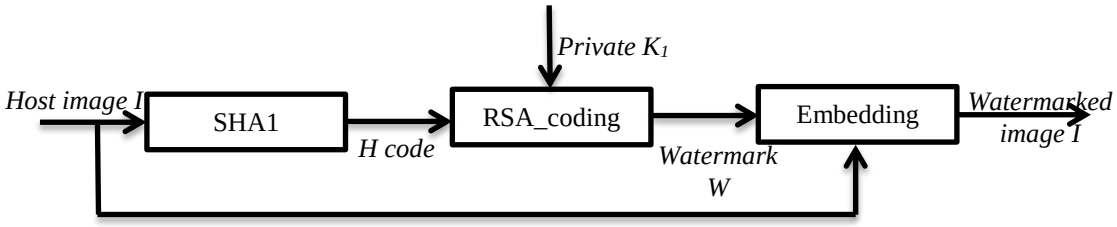

Fig. 2. Watermark embedding

In the first step of algorithm, we apply hash function SHA1 into a host image I to obtain the hash code denoted *H*. H is a bit array of 512. Then we manipulate the RSA coding algorithm taking H code and private key K_1 as inputs, the output is watermark W. Finally, we get the watermarked image by employing the embedding procedures shown in Table 2 or Table 3.

4.2 Authentication procedure

The watermarked image I' may be attacked by different operations in transmission. Subsequently, the receiver obtains an attacked image I^*. The determining the integrity of the image I^* is shown in the fig. 3.

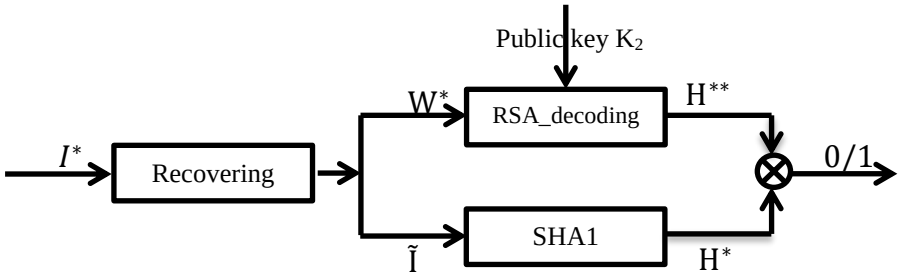

Fig 3. Authentication process

The fig.3 presents that, at first extracted watermark W^* and recovered image $\tilde{I}$ are restored from image I^* by using the recovering procedure in Table 2 or Table 3 in section 2.2. Next, we apply the hash function SHA1 into image $\tilde{I}$ to get the hash code H^*. The RSA decoding algorithm then is used with public key K_2 as an input, its output is hash code H^{**} decrypted from watermark W^*. In the last step, H^* is compared to H^{**}, if $H^* = H^{**}$ then we conclude that the watermarked image I' is integrity otherwise the watermarked image I' was attacked illegally. Since the watermark is representative of the whole image and is defined by the hash function, every tiny change of pixels will result in the different hash code. Therefore, the proposed watermarking scheme is able to detect any tiny changed pixels.

5 Conclusion

This paper introduces the algorithms with linear complexity regard to the length of vector to check the expandability and changeability of a vector based on Alattar and Weng's methods. As a result, both of the procedures of embedding and extracting are speeded up as well as the embedding capacity is higher. This improvement is extremely important for watermarking systems in practical, when ones often have to work with large-scale vectors and large size of watermarks. The experimental results showed that the scheme using the proposed expandable and changeable criteria is much better than the others in terms of computational complexity and embedding capacity. Moreover, the public key reversible watermarking based on the two procedures is able to detect any unauthorized attacks on watermarked images.

References

[1] Adil Haouzia and Rita Noumeir, Methods for image authentication: a survey, *Multimed. Tools Appl,*, **39** (2008), 1-46. https://doi.org/10.1007/s11042-007-0154-3

[2] Asiffullad Khan, Ayesha Siddia, Summuyya Munib and Saan Ambreen Malik, A recent survey of reversible watermarking techniques, *Information Sciences*, **279** (2014), 251-272. https://doi.org/10.1016/j.ins.2014.03.118

[3] A.M. Alattar, Reversible Watermarking Using the Difference Expansion of A Generalized Integer, *IEEE Transactions on Image Processing*, **13** (2004), 1147–1156. https://doi.org/10.1109/tip.2004.828418

[4] C.C. Lee, H.C. Wu, C.S. Tsai and Y.P. Chu, Adaptive lossless steganographic scheme with centralized difference expansion, *Patterm Recognition*, **41** (2008), 2097-2106. https://doi.org/10.1016/j.patcog.2007.11.018

[5] J. Tian, Reversible data embedding using a difference expansion, *IEEE Trans. Circuits Syst. Video Technol*., **13** (2003), 890–896. https://doi.org/10.1109/tcsvt.2003.815962

[6] K.Y. Mohammad and A.J. Ahmed, Reversible Watermarking Using Modified Difference Expansion, *International Journal of Computing & Information Sciences*, **4** (2006), no. 3, 134-142.

[7] M. Khodaei and K. Faez, Reversible Data Hiding By Using Modified Difference Expansion, *2nd International Conference on Signal Processing Systems*, (2010). https://doi.org/10.1109/icsps.2010.5555649

[8] D.M. Thodi, J.J. Rodriguez, Expansion embedding techniques for reversible watermarking, *IEEE Transactions on Image Processing*, **16** (2007), 721-730. https://doi.org/10.1109/tip.2006.891046

[9] Chi Man Pun, Ka Cheng Choi, Generalized integer transform based reversible watermarking algorithm using efficient location map encoding and adaptive thresholding, *Computing*, **96** (2014), no. 10, 951–973. https://doi.org/10.1007/s00607-013-0357-6

[10] Xiang Wang, Xiaolong Li, Bin Yang and Zongming Guo, Efficient Generalized Integer Transform for Reversible Watermarking, *IEEE Signal Processing Letters*, **17** (2010), 567-570. https://doi.org/10.1109/lsp.2010.2046930

[11] G. Xuan, C. Yang, Y. Zhen, Y.Q. Shi and S. Ni, Reversible data hiding based on wavelet spread spectrum, *IEEE International Workshop on Multimedia Signal Processing*, (2004), 211-214. https://doi.org/10.1109/mmsp.2004.1436530

[12] D. Coltuc and J-M. Chassery, Very Fast Watermarking by Reversible Contrast Mapping, *IEEE Signal Processing Letters*, **14** (2007), 255-258. https://doi.org/10.1109/lsp.2006.884895

[13] Bo Ou, Xiaolong Li, Yao Zhao, Rongrong Ni and Yun-Qing Shi, Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding, *IEEE Transactions on Image Processing*, **22** (2013), no. 12, 5010-5021. https://doi.org/10.1109/tip.2013.2281422

[14] Xiaolong Li, Bin Yang and Tieyong Zeng, Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection, *IEEE Transactions on Image Processing*, **20** (2011), no. 12, 3524-3533. https://doi.org/10.1109/tip.2011.2150233

[15] Dinu Coltuc, Adrian Tudoroiu, Mutilbit versus multilevel embedding in high capacity difference expansion reversible watermarking, *20th European Signal Processing Conference*, (2012).

[16] Shaowei Weng, Chu Chuan Chu, Nian Cai and Rongxin Zhan, Invariability of mean value based reversible watermarking, *Journal of Information Hiding and Multimedia Signal Processing*, **4** (2013), 90-98.

[17] K. Wang, Y.J. He and Z.M. Lu, A high capacity lossless data hiding scheme for JPEG images, *Journal of Systems and Software*, **86** (2013), 1965-1975. https://doi.org/10.1016/j.jss.2013.03.083

Received: April 26, 2017; Published: May 25, 2017