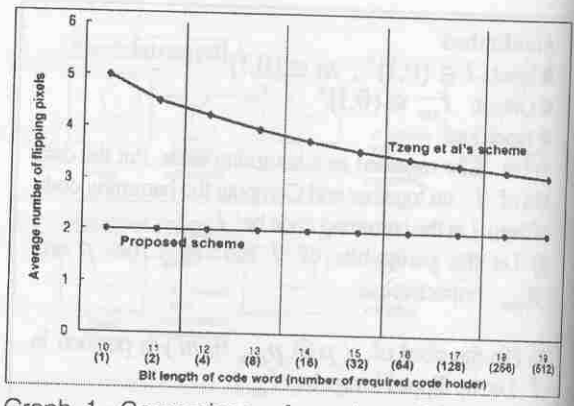
pixels to be flipped is 2 because two pixels are flipped. Since the number of other images that contain the same watermark is $2^{c-\log_2(c+1)-1}$. Thus, the false positive ratio of the proposed scheme is $2^{c-\log_2(c+1)-1}/2^c \approx c^{-1}$.

4.3 Performance comparison between Tzeng et al's scheme the proposed scheme

This subsection provides a simple comparison result between the proposed scheme and Tzeng et al's scheme. We assume that the bit length of the cover image is 1024bit. In this case, the false positive ratio of the proposed scheme is fixed to $1/1024 \approx 9.7\times10^{-4}$ and the number of flipped pixels in the proposed scheme is two. The following graph shows that Tzeng et al's scheme requires flipping more pixels than the proposed one to achieve the same false positive ratio as the proposed one. In Graph 1, if the codeword bit length is 10bit and the number of code holder is 1, the false positive ratio of Tzeng et al's scheme is the same as the proposed scheme. In this case, the average number of flipping pixel is 5. If the length of the codeword bit is longer, the required average number of flipping pixel decreases in Tzeng et al's scheme. But the number of required code holder increases exponentially if the codeword length increases linearly in Tzeng et al's scheme. Thus, to make the number of flipping pixel be the same as the proposed scheme, Tzeng et al's scheme requires extremely many code holders. For example, in Graph 1, if the code word length is 19-bit, 512 code holders are required; this means that the stego image generator and the verifier must share 512*19=9728 bits. Moreover, in this case, the average number of flipping pixel is 3.13, which are still far more than that of the proposed scheme. If the size of the cover image is bigger, the gap between the proposed scheme and Tzeng et al's increases because the codeword length in Tzeng et al's scheme should be longer to make the false positive ratio be the same as the proposed one.

5. Conclusion

In the paper, a novel fragile watermarking scheme for binary image is proposed. The proposed scheme needs relatively small number of flipping pixels with preserving moderate false positive ratio. We show that the required number of flipping pixels to embed a watermark in the proposed scheme is smaller than in Tzeng et al's scheme for both schemes to have the same false positive ratio with the analysis results of both schemes.



Graph 1. Comparison of number of flipping bits when the false positive ratio is fixed.

Acknowledgement

This work was supported by Brain Korea 21 Project, The school of information technology, KAIST in 2006.

References

[1] C. Tzeng, and W. Tsai, "A New Approach to Authentication of Binary Images for Multimedia Communication with Distortion Reduction and Security Enhancement", *IEEE Communications Letters*, 7(9):443-445, Sep. 2003.

[2] T. Downey, Calculating the Hamming Code, Available: http://www.cs.fiu.edu/~downeyt/cop3402/hamming.html, 2004.

[3] R. Crandall, "Some Notes on Steganography", posted on Steganography Mailing List, 1998.

[4] A. Westfield, "High Capacity Despite Better Steganalysis (F5-A Steganographic Algorithm)," in Proc. *Information Hiding. 4th International Workshop*. LNCS, vol. 2137, Springer-Verlag, pp. 289-302, 2001.

[5] F. Galand, G. Kabatiansky, "Information hiding by coverings", In Proc. *ITW2003*, Paris, France, pp. 151-154, 2003.

[6] J. Fridrich and D. Soukal, "Matrix Embedding for Large Payloads," in Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, San Jose, CA, January 16-19, pp. W1-W15, 2006.

[7] Min Wu, and Bede Liu, "Data Hiding in Binary Images for Authentication and Annotation", IEEE Transactions on Multimedia, Vol. 6, No. 4, pp. 528-538, August 2004.

[8] Y. Tseng, Y. Chen, and H. Pan, "A Secure Data Hiding Scheme for Binary Images", IEEE Transactions of Communications, vol. 50, No. 8, pp. 1227-1231, 2002.

A Fragile Watermarking Scheme For Binary Image Authentication using Hamming code

Younho Lee*, Heeyoul Kim*, Byungchun Chung*, Yongsu Park, and Hyunsoo Yoon***

*** Division of Computer Science, EECS Department, KAIST**

373-1, Guseong dong, Yuseong gu, Daejeon, Korea.

**** School of Information and Communication, Hanyang University, Korea**

{yhlee, hykim, bcchung}@nslab.kaist.ac.kr, yspark@hanyang.ac.kr, hyoon@kaist.ac.kr

ABSTRACT

A fragile watermarking aims to detect any accidental or malicious image alteration. This paper proposes a new fragile watermarking scheme for binary image authentication. By the proposed scheme, the watermark can be inserted in the binary image minimizing the image distortion with moderate false positive ratio which means the probability that the falsely modified image can pass the verification test. With the help of the watermark embedding technique based on the hamming code, the proposed scheme can embed the $\lceil \log_2(c+1) \rceil$-bit watermark on c-bit binary host image by only flipping two pixels of the host image. Because of the image distortion caused by inserting the watermark is very small, the adversary can hardly detect whether the image has watermarks or not. We compare the proposed scheme to the Tzeng et al's approach with the following two factors: the number of flipping pixels to embed the watermark and the false positive ratio.

Keywords : Fragile watermark, Information Hiding, Security

1. Introduction

With the rapid growth of IT technology, the digital media prevails through the world. Compared with analogue media, the digital media has many advantages. However, some security problems have risen such as ease of making an illegal copy and fabricating the digital media. To prevent such security problems, the digital watermarking is useful. The digital watermarking is used to insert a sequence of bits in the digital media so as to make an assertion about the digital media in the future.

The digital watermark can be classified as the robust watermark or the fragile one. The robust watermark is used as a copyright assertion or finger-print of digital media. It should not be easily removed even if the digital media is all or a part of it is altered. On the other hand, the fragile watermark can be easily removed by even very small alteration of the digital media. This fragility helps to achieve the main objective of the fragile watermark because the fragile watermarking technique aims to check the integrity or authenticity of the digital media; if the watermark is removed, it can be simply concluded that the digital media is corrupted.

Recently Tzeng et al. have proposed a fragile watermarking scheme for binary images [1]. Unfortunately, it has relatively high false positive ratio, which means the probability that the falsely modified image can pass the verification test.

In this paper, a novel approach of the fragile watermarking for binary images is proposed. The propose scheme employs the hamming code based watermark embedding technique to minimize the number of flipping pixels in the host image when the watermark is embedded in the host image [3-5]. With the help of this new embedding technique, the watermark of $\lceil \log_2(c+1) \rceil$ bit length can be embedded to the c-bit host image by flipping only 2 pixels. Thus, the watermark generated by the proposed scheme can be more undetectable than that by Tzeng et al's approaches [1].

The organization of this paper is as follows. Section 2 and Section 3 present the related work and motivation, and the new fragile watermarking scheme respectively. The performance comparison between the proposed scheme and some of previous works is shown at Section 4. Finally, the conclusion is given in Section 5.

2. Related work and Motivation

The watermarking technique can be regarded as a kind of the digital hiding because it embeds a sequence of bits in the host image. During last years, a number of data hiding schemes for binary images have been proposed. Tseng et al. [7] and Wu et al. [8] proposed new data hiding schemes respectively. These schemes aim to enhance the capacity of the embedded image, small perceptual distortion of the host image, and the reliable transmission of the embedded data. However, they don't treat enough the authenticity and integrity of the host image because the reliable transmission of the hidden data is more considered in their works. On the other hand, Tzeng et al. [1] proposed a scheme to provide the authenticity and integrity of the host image. So it does not aim to provide large capacity and strong reliability of the embedded data but the way to detect the alteration of the host image with small image distortion caused by inserting the watermarks. This paper deals with the latter case. The motivation of this work is to suggest a new fragile watermarking scheme providing the higher false positive ratio with smaller host image distortion caused by the insertion of the watermark..

2. Proposed scheme

A new fragile watermarking scheme is presented in this section. The proposed scheme contains the stego image generation algorithm and the stego image verification algorithm. In the stego image generation, the watermark is embedded in the host image, which is called as cover image also. After embedding, the watermark is hided using the watermark concealing algorithm. The image which includes the concealed watermark is called as stego image. In the proposed scheme, the same key $K \in \{0,1\}^t$ (t is security parameter) is used for both embedding and extracting the watermark. K should be known to only the stego image generator and the stego image verifier and should not be revealed to others. An overview of the basic scheme is depicted in Figure 1. In the figure, the bit length of the cover image and the stego image is c, and the bit length of the watermark is $\lceil \log_2(c+1) \rceil$. It is assumed that the stego image generator and verifier have the pseudo random function $f_a : \{0,1\}^t \rightarrow Z_a$. The detailed description of each algorithm is given at each subsection.

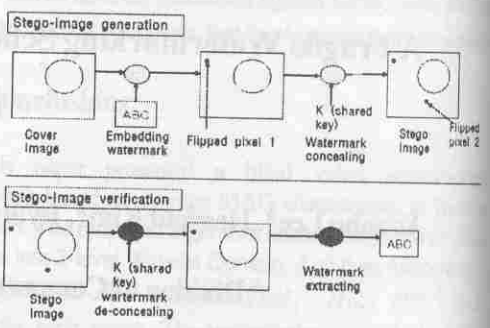


Figure 1. Overview of proposed scheme

3.1 Stego image generation

The procedure of the basic stego image generation algorithm is divided into two sub algorithms: the watermark embedding and the watermark concealing. We employ the embedding algorithm based on the hamming code **(AuthEmbed)** [3-5] for the watermark embedding. In **AuthEmbed**, the cover image I is transformed to a watermark embedded image I_{em}. The watermark concealing sub algorithm **(AuthHide)** changes a pixel of I_{em} so as to conceal the watermark. **AuthHide** outputs the stego image I_{stego}. The result of this algorithm makes anyone who does not have the shared secret key K cannot extract the watermark m. The detailed description of each sub algorithm is as follows. Since **AuthHide** algorithm is only the reverse procedure of **AuthDeHide** which is used in the Stego image verification algorithm, both algorithms are described in the same box.

Because the hamming code is a perfect code, flipping only one pixel is enough to hide the watermark. An easy explanation of computing hamming code is given at [4].

3.2 Stego image verification

The stego image verification algorithm consists of the watermark de-concealing sub algorithm (**AuthDeHide**) and the watermark extraction sub algorithm (**AuthDeEmbed**). **AuthDeHide** is the reverse of **AuthHide**. The description of **AuthDeHide** is given below. As we mentioned above, **AuthDeEmbed** is the hamming-code-based extraction algorithm [3-5]. The procedure of the sub algorithm is shown below too.

AuthEmbed
- Input: $I \in \{0,1\}^c$, $m \in \{0,1\}^{\lceil \log_2(c+1) \rceil}$
- Output: $I_{em} \in \{0,1\}^c$
- Procedure

1) Let I be regarded as a hamming code. Put the data bits of I on together and Compute the hamming code of them. Let the hamming code be I_{ham}.
2) Let the parity bits of I and I_{ham} be p and p_{ham} respectively.
3) Flip the pixel of $(p \oplus p_{ham} \oplus m)$-th position in I. Let the flipped image be I_{em}.
4) Return I_{em}.

AuthHide (AuthDeHide)
- Input: $I_{em}(I_{stego}) \in \{0,1\}^c$, f_c, $K \in \{0,1\}^t$
- Output: $I_{stego}(I_{em}) \in \{0,1\}^c$
- Procedure

1) Flip the pixel of $f_c(K)$ -th position in $I_{em}(I_{stego})$.
2) Return $I_{stego}(I_{em})$.

AuthDeEmbed
- Input: $I_{em} \in \{0,1\}^c$
- Output: $m \in \{0,1\}^{\lceil \log_2(c+1) \rceil}$
- Procedure

1) Let I_{em} be regarded as a hamming code. Put the data bits of I_{em} on together and Compute the hamming code of them. Let the hamming code be I_{ham}.
2) Let the parity bits of I_{em} and I_{ham} be p_{em} and p_{ham} respectively.
3) Return $m = (p_{em} \oplus p_{ham})$

4. Performance Analysis

In this section, the performance of the proposed scheme is compared with that of Tzeng et al's work [1]. The following two measurement metrics are used to the comparison.

- Number of flipping pixels: it means the required number of flipping pixels to embed the watermark in the cover image. The number of flipped pixels should be minimized to preserve the quality of the cover image.
- False positive ratio: it means the probability that the false stego image which is different from the original one can pass the stego image verification test.

In the first subsection, the analysis of Tzeng et al's work is described and the second subsection presents the analysis of the proposed work, and the final subsection provides the comparison result between two schemes.

4.1 Analysis of Tzeng et al's scheme

It is first assumed that the codeword length is k and the number of code holders is q. Let the code words of which the number is q, select the result bits on the uniform distribution. The final assumption is that the cover image is divided into N blocks and the bit length of the cover image is c.

In Tzeng et al's scheme, authentication codes $c_1,\ldots,c_N$ are selected with one secret key, which is shared with the image verifier, and the code holders are generated with another secret key. If $c_1,\ldots,c_N$ are selected on the uniform distribution, the number of bits included in the cover image is kN bits. The derivation procedure of the average number of flipping pixels in each block on embedding the authentication codes is as follows.

For any c_i $(i \in \{1,\ldots,N\})$, let the k-bit strings that the q code holders selects be $t_1,\ldots,t_q$. Then the number of flipping pixels in block i is the smallest hamming distance between c_i and $t_1,\ldots,t_q$. If $t_1,\ldots,t_q$ are uniformly selected in $[0,2^{c/N-1}]$, the probability distribution of the hamming distance between each of $t_1,\ldots,t_q$ and c_i is the binomial distribution. Based on this, it can be easily derived the probability distribution of the hamming distance between c_i and the one, that has the smallest hamming distance from c_i among $t_1,\ldots,t_q$. Thus, the average number of flipping pixels in each block has been described as follows.

(Average number of flipping pixels) =

$$\sum_{i=1}^{k} i * (A_i - A_{i-1})$$

(Where $A_l = 1 - (2^{-k} \sum_{j=l+1}^{k} \binom{k}{j})^q$

The average number of flipping pixels in the cover image is N * (Average number of flipping pixels). Now we discuss the false positive ratio. In each block, even if all pixels can be altered except the pixels which include the code word, the stego image can pass the verification test. Further, if the block is modified with making the code word be another position instead of the original one, the overall stego image passes the verification test. Considering the above cases, the false positive ratio of Tzeng et al's scheme is as follows. Since the authentication code is inserted and verified per each block independently; no relation between the authentication codes in different blocks, the false positive ratio of one block is the same as that of the stego image.

(False positive ratio) = $\sum_{i=1}^{q} (-1)^{i+1} \binom{q}{i} 2^{-ik}$

4.2 Analysis of the proposed scheme

In the proposed scheme $\lceil \log_2(c+1) \rceil$-bit watermark can be embedded in the c bit cover image. The required number of