Multiuser-based shadow watermark extraction system

Feng-Hsing Wang a, Kang K. Yen b, Lakhmi C. Jain a, Jeng-Shyang Pan c,*

a School of Electrical and Information Engineering, University of South Australia, Australia
b Department of Electrical and Computer Engineering, Florida International University, USA
c Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, Taiwan, ROC

Received 17 March 2005; received in revised form 13 August 2006; accepted 26 December 2006

Abstract

A new watermarking scheme having the ability of sharing secret with multi-users is proposed. It splits the original watermark into two shares and embeds one share into the cover image to increase the security. A polarization procedure is performed to establish a polarity stream from the cover image. The second share and the polarity stream are used to generate a master key and several normal keys. In this system, only the super-user can reveal the genuine watermark directly. Other users possess the normal keys can obtain shadow watermarks merely. By combining the shadow watermarks together, the real watermark can be recovered.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Watermarking; Visual cryptography (VC); Key design

1. Introduction

With the widespread use of Internet and the rapid development of computer technology, transferring digital data via Internet has become a common activity nowadays. Due to the digital nature of easy modification, fast transferring, and unlimited copying, the solutions for tempering verification, copyright protection, and ownership demonstration are getting more and more urgent in recent years. Among the techniques, digital watermarking technique [1,8,21,22] has been considered as one of the solutions for those problems mentioned.

A variety of watermarking methods has been proposed [6,9,10,13]. Currently, most of researchers are concentrated on the transform-based watermarking schemes, such as the discrete cosine transform (DCT) [2,4] and the discrete wavelet transform [5,11], since they provide better performance than the schemes based on spatial domain. Considering the applications of watermarking systems, some of them provide better imperceptibility and others focus on other benchmarks like robustness or embedding capacity.

In the area of applying watermarking techniques to implement secret-sharing systems for multi-users, we found that few researchers have explored this field. Therefore, in this paper we focus on the security of the...
hidden secret information and propose a new image-based watermarking system for sharing the secret with multi-users. Instead of embedding the original watermark into the cover image like general watermarking systems, our system splits the original watermark into two shares, embeds one share into the cover image, and uses another share for the proposed key generating procedure. With the aids of the proposed system, the user possesses the unique master key can reveal the genuine watermark directly. Otherwise, a shadow watermark can be obtained merely. We implement this system by applying the DCT-based watermarking algorithm [15] and the vector-quantisation-based watermarking algorithm [11], and the experimental results demonstrate the effectiveness of the proposed system.

1.1. Visual cryptography (VC)

To share secret among multi-users, visual cryptography (VC) [12] is a well-known image-based scheme. Generally speaking, for a secret to be shared with \( n \) users, the scheme first transforms the secret into image format, and splits this image into \( n \) meaningless shares. Each share is printed on a transparent slide and assigned to each user afterwards. To reveal the secret, the necessary amount of shares has to be presented. That is, by stacking these shares, the secret can be revealed visually without any mathematical calculation. An example of a \( n = 2 \) case is given in Fig. 1.

1.2. VC-based watermarking methods

Introducing VC into watermarking systems is not a new idea, however, the existing watermarking systems [3,16,17] only apply the concept of splitting the original watermark to increase the security of the systems. The other significant feature such as secret sharing, is not taken into account. The description below illustrates how a general VC-based watermarking scheme works.

For a general image-based watermarking system, the original watermark (such as in Fig. 1(a)) is usually embedded into the given cover image directly to form a watermarked image. VC can be applied to split the original watermark into two shares (such as in Fig. 1(b) and (c)) before embedding so as to increase the security. The first share is embedded into the cover image and the second share is regarded as a key. The extracted content will be meaningless to the extractor without this key. This therefore increases the security of the embedded information.

Another application of such systems is ownership verification. That is, if a meaningful image can be obtained by stacking the extracted watermark with the key, the ownership of this watermarked image therefore can be determined.

2. Proposed watermarking system

The structure of the proposed watermarking system is depicted in Fig. 2 and its steps are listed below. Details of the methods for implementation are given in the following sections.

---

**Fig. 1.** The example of a traditional VC scheme: (a) the secret image, (b) the generated first share, (c) the generated second share, and (d) the result of stacking the two shares.
In Fig. 2, let $W$ be a watermark, a secret to be shared with $n$ users, $X$ be a cover image to carry the information of $W$, and $X_0$ be the watermarked image which contains the information of $W$, and $K_0$ and $\{K_1, K_2, \ldots, K_n\}$ be the keys for revealing the information hidden in $X'$. To hide $W$ into $X$ and to generate these keys, the four steps are as follows:

(i) Split the original watermark $W$ into two shares $S_1$ and $S_2$ by applying the method presented in Section 3.1.
(ii) Embed share $S_1$ into the cover image $X$ so that a watermarked image $X_0$ can be obtained. The details are described in Section 3.2.
(iii) Establish a polarity stream $P$ from $X_0$ by employing either method presented in Section 3.3.
(iv) Generate the unique master key $K_0$ and $n$ normal keys $\{K_1, K_2, \ldots, K_n\}$ from $S_2$ and $P$. Section 3.4 describes the details.

The keys generated with a copy of the watermarked image $X_0$ are then assigned to the related users to share the secret $W$ hidden in $X'$.

To obtain the watermark, which may be the original watermark or a shadow watermark, from the watermarked image $X$, which may be the original watermarked image $X_0$ or an image modified from $X_0$, the steps are as follows:

(i) Extract a shadow watermark $\tilde{S}_1$ from $\hat{X}$ by using the method illustrated in Section 3.2.
(ii) Establish a polarity stream $\hat{P}$ from $\hat{X}$ by applying the method described in Section 3.3.
(iii) Generate a watermark $W_i$, where $0 \leq i \leq n$, from $\tilde{S}_1, \hat{P}$, according to the key $K_i$ used. If $K_i$ is a master key (i.e., $i = 0$), then $W_i$ is the original watermark. Otherwise, $W_i$ is a shadow watermark. Step (iv) is then used to recover the original watermark.
(iv) Combine all the shadow watermarks extracted to recover the original watermark. The method presented in Section 3.5 explains this step.

3. Implementation methods

Generally speaking, to implement the proposed watermarking system, the choice of the watermarking algorithm or the splitting algorithm is not limited. Any suitable method proposed in the literature can be
(vi) The architecture of the proposed watermarking system is an open issue. Either part of the system can be replaced by other parts which provide similar functions, for example, replacing the watermarking procedure by other available method, as mentioned in (v). This means the system is easy to be implemented according to the purposes and concerns of the users.

(vii) In some cases the question of key delivery is concerned, but it is beyond the focus of this paper.

(viii) In the watermark splitting step, the process of watermark extraction can be employed to implement the process of feature selection. In this condition, parameter $a$ will be 1 and the content of the cover image will not be altered, because the watermark bits to be embedded are the same as the ones extracted from the cover image. The information of the original watermark is only contained in the generated keys. This is named zero-watermarking in some papers.

(ix) Since $R$ is adjustable, it is reasonable to select a suitable $R$ to have better performance in imperceptibility and/or robustness.

7. Conclusion

In this paper, the concept of hierarchical keys has been introduced into the watermarking system such that different users with different security status obtain different information. The super-user with the unique master key can reveal the genuine secret directly, but the normal users with the normal keys can only obtain shadow watermarks. By combining their shadow watermarks, the secret can be revealed. Unlike some schemes which embed all the shadow watermarks into the cover image, the proposed scheme only embeds one share. It therefore provides better visual quality than others. Especially, the robustness against some attacks is good enough even with the attack of a high JPEG compression rate (quality factor is 30%). In conclusion, the proposed system is novel, effective, as shown in the experimental results.

References


