Human-Machine Identification Using Visual Cryptography

Mi-Ra Kim* Ji-Hwan Park* Yuliang Zheng**

* Dept of Computer Science, PuKyong National University,
599-1 Daeyeon-Dong, Nam-Ku, Pusan 608-737, Korea
{kimmr,jhpark}@unicorn.pknu.ac.kr
** School of Comp & Info Tech, Monash University
McMahons Road, Frankston, VIC 3199, Australia
yuliang@pscit.monash.edu.au

ABSTRACT

In this paper we investigate human identification schemes using visual cryptography, which have a desirable property of decoding concealed images without any computationally expensive cryptographic operations. Main contributions of this work include: (1) we generalize a visual secret sharing scheme which is originally proposed by T.Katoh and H.Imai and can conceal only two query images into a display image, into a scheme that can conceal a multiple number of query images. (2) By the use of a technique proposed by Droste, we further extend the gener-alized scheme so that every combination of the transparencies can conceal independent secret images.

1. Introduction

Due to the widespread use of information and communication technologies, it is increasingly frequent for a human user to authenticate him or herself to a physical terminal such as an ATM and a computer, in order to obtain services provided by a computing and communication system. The problem involved in the authentication process is commonly called the *human identification* problem. Over the years, various human identification schemes have been proposed to verify whether a user is indeed who he or she claims to be. Currently, most of these schemes are based on passwords. Although a password based scheme is simple to use, past experience shows that it is inherently weak against peeping and eavesdropping attacks.

In [1], an interactive human identification scheme was proposed to overcome the weaknesses. With this scheme, multiple rounds of challenge-and-response take place between a human user and a terminal. To answer a question posted by the terminal, the user is generally required to perform a simple computational task. Analysis shows that such an interactive scheme is much stronger than a password based one in terms of resistance against peeping, although most people will find the scheme unacceptable due to the need of computation by a user.

In another line of research, T.Katoh and H.Imai proposed an interesting scheme which uses slides generated by visual cryptography [2] as against queries in an interactive human identification scheme [3]. With a visual cryptography based scheme, a pre-made slide is distributed to a user. By stacking a slide to a query image (display image) shown on the screen of a terminal, the user can be sure whether the terminal is a "good" or otherwise "bad" one, prior to providing a password to the terminal. The scheme can provide multiple identification by distributing several slides to a user, each revealing a different query image when stacked to the same display image.

In this paper, we generalize Katoh and Imai's scheme so that it can conceal several query images. In addition we propose a new construction method by the use of Dorset's technique [4]. In section 2, we introduce the basic model of visual cryptography proposed by M.Naor and A.Shamir. In section 3, we review briefly a human identification scheme using visual cryptography proposed by Katoh and Imai, and propose the generalized method, which can conceal several query images in a single display image. In the same section, a further extended method is proposed in which a group of slides can conceal an independent secret image.

2. Basic Model of Visual Cryptography

The simplest version of the visual secret sharing problem assumes that a binary image is composed of a collection of black and white pixels and each pixel is handled separately. Each pixel of the original image may appear in *n* modified versions, each of which consists of a collection of *m* black and white sub-pixels, called a “share”. Each share can be "stored" on (photo-copied to) an ordinary plastic transparency.

The resulting structure can be described by a $n \times m$ Boolean matrix $S = [s_{i,j}]$ for each original pixel, where $s_{i,j} = 1$ if and only if the j th sub-pixel in the i th transparency is black and $s_{i,j} = 0$ if and only if the sub-pixel is white. When transparencies are stacked together in a way, which properly aligns the share, we see a combined share whose black sub-pixels are represented by the Boolean "or" of rows in the matrix S . The grey level of this combined share is proportional to the Hamming weight $H(V)$ of an "or"ed m-vector V . This grey level is interpreted by the visual system of a user as black if $H(V) \geq d$ and white if $H(V) \leq d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. What follows is a formal definition of a visual secret sharing scheme.

Table 1. Row Vectors for the Display Image

The combination of pixel values			Vector for display image	
Query image1	Query image2	Query image 3	Identity matrix(I)	Zero matrix(Z)
W	W	W	1 1 1	0 0 0
W	W	B	1 1 0	1 0 0(0 1 0, 0 0 1)
W	B	W	1 0 1	1 0 0(0 1 0, 0 0 1)
W	B	B	1 0 0	1 1 0(1 0 1, 0 1 1)
B	W	W	0 1 1	0 0 1(0 1 0, 1 0 0)
B	W	B	0 1 0	0 1 1(1 0 1, 1 1 0)
B	B	W	0 0 1	0 1 1(1 0 1, 1 1 0)
B	B	B	0 0 0	1 1 1

[Definition] A visual (k,n) secret sharing scheme consists of two collections of $n \times m$ Boolean matrices C_0 and C_1. To share a white pixel, a dealer chooses at random one of the matrices in C_0, and to share a black pixel, chooses again at random one of the matrices in C_1. Each row of a chosen matrix corresponds to a share, and if each element value of a row is 1, it represents a black, if 0, it represents a white. The solution of the visual (k,n) secret sharing scheme is considered valid if the following three conditions are satisfied;

1. For any S_0 in C_0, the "or" V of any k of the n rows satisfies $H(V) \leq d - \alpha m$.
2. For any S_1 in C_1, the "or" V of any k of the n rows satisfies $H(V) \geq d$.
3. For any subset $\{i_1, i_2, \cdots i_q\}$ of $\{1,2,\cdots n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for $t \in \{0,1\}$ obtained by restricting each $n \times m$ matrix in C_t (where $t \in \{0,1\}$) to rows $i_1, i_2, \cdots i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Conditions 1 and 2 are related to "contrast" in a reconstructed image by way of stacking shares, and Condition 3 is about "security" in that one cannot decide whether a share pixel is white or black by inspecting fewer than k shares.

3. Human identification scheme using visual cryptography

Human identification scheme using visual cryptography [3] proposed by Katoh and Imai could conceal two query images in a display image. With this scheme a different query image is resulted when a different pre-distributed slide is stacked on a display image. It is this property that ensures that a terminal and a user can mutually identify each other. The procedure for their human identification is as follows.

[Procedure of verification]

1. A user is associated with an identity (ID). Similarly, a terminal has an ID. The user and the terminal have

a shared secret. A dealer distributes slides to the user. The slides are constructed by a share generating matrix which is defined in a visual (2,2) secret sharing scheme.

2. The user provides his or her ID to the terminal in order to obtain a service.
3. The terminal shows a displayed image on the screen. Then the user stacks one of his or her slides on the screen, which reveals a message.
4. A user carries out a simple operation by the use of the message in conjunction with the shared secret information. He or she then provides the terminal with the outcome of the operation.

As one can see, the human identification process can interactively verify a user and a terminal by the use of slides.

3.1 Generalized construction method

As an extension of Katoh and Imai's scheme, we propose a generalized construction method which can conceal several query images in a displayed image. First, a new share generating matrix is obtained by the following method:

- I : the $n \times n$ Identity matrix
- Z : the $n \times n$ Zero matrix (all element is 0)
- IZ : Concatenation of I and Z, the $n \times 2n$ user's share generating matrix
- C : the collection obtained by permuting the columns of the user's share generating matrix IZ .

For example, a collection of the share generating matrix of user C in the case of $n = 3$ is

$$C = \left\{ \begin{array}{l} \text{all the matrices obtained by permuting} \\ \text{the columns of} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \end{array} \right\}.$$

We then choose any one of the collections of the share generating matrix C to construct the user's slides. The first row is used for the user's slide 1, the second for slide 2, and the third for slide 3.

In order to generate a slide for a display image to be shown on the screen of a terminal, we consider separating the user's share generating matrix IZ into identity matrix part I and zero matrix part Z , and that each row of matrix IZ corresponds to each query image in turn. In the identity matrix part I , when a pixel of all query images is black, we perform the "and" operation for corresponding row vectors, otherwise we perform the "or" operation. For example, if the pixel values of query images 1, 2 and 3 are all white (WWW), we can obtain "111" which is the "or"-ed value of the 1, 2 and 3 rows in I . Whereas in the zero matrix part Z , we change 0 to 1 as many as the number of black pixels B_k in the combination of pixel values of query images. The number of combination is ${}_nC_{B_k}$. Table 1 describes a constructing example of a row vector for a display image when $n = 3$. Fig.1 shows the procedure which decodes each pixel (B/W) on the display image using the vector for the display image in Table 1. When "or"ing user's shares corresponding to each row of C and a vector (010011) for the display image, we can recognize that a share of the decoded image is BWB . If the user stacks 3 slides to the displayed image alternately, it is possible to decode the 3 query images. When the Hamming weight is $w = 3$, the share is recognized as white, and when the weight is $w = 4$, the share is recognized as black. Furthermore, if the Hamming weight of the share is n , we can recognize it as white, and if the Hamming weight of the share is $n+1$, we recognize it as black for the relative difference $\alpha = 1/2n$. One can observe that the size of share m becomes 2 times the number of the query image n .

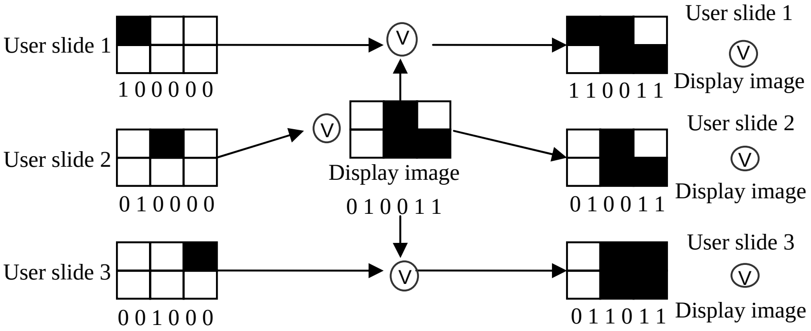


Fig. 1. Stacking of User's Share on the Displayed Image

3.2 The extension of Droste’s scheme for Human Identification

Table 2. Row Vectors for Display Image in the Proposed Scheme

The combinations of pixels			Row vector for the display image	
			Matrix group I	Matrix group II
Query image 1	Query image 2	Query image 3	0 0 1 1 0 1 0 1	0 1 1 1 1 0 1 1
W	*W*	*W*	0 1 1 0	1 1 0 0
W	*W*	*B*	0 1 1 0	1 0 0 1
W	*B*	*W*	0 1 1 0	0 1 1 0
W	*B*	*B*	0 1 1 0	0 0 1 1
B	*W*	*W*	1 0 0 1	1 1 0 0
B	*W*	*B*	1 0 0 1	1 0 0 1
B	*B*	*W*	1 0 0 1	0 1 1 0
B	*B*	*B*	1 0 0 1	0 0 1 1

Although Katoh and Imai’s scheme can decode to a different query image by stacking any one of a user's slides to the displayed image, all query images overlap one another when stacking user slides to the displayed image. This reduce the resolution of the scheme. To overcome this problem, by applying Droste’s scheme, we propose a new construction method. With the new method, every combination of the slides can conceal an independent query image.

First, in order to conceal n query images in one displayed image, we define a matrix group I and a matrix group II , and construct a set of share generating matrices of a user.

◆Matrix group I

- $G_{n-1}(\mathrm{I})$: the matrix combined with $M_{n-1,i}$, $0 \le i \le n-1$
- $M_{n-1,i}$: consists of $n-1$ rows and all columns of i 1’s

◆Matrix group II

- $G_{n-1}(\mathrm{II})$: the matrix combined with $M_{n-1,i}$ which consists of all columns of $n-2$ 1’s and ${}_{n-1}C_{n-2}$ columns of only 1’s.

For example, when $n=3$,

$$G_2(\mathrm{I}) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad G_2(\mathrm{II}) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

A collection of a user's share generating matrices, which is obtained by concatenation of $G_{n-1}(\mathrm{I})$ and $G_{n-1}(\mathrm{II})$, C is

$$C = \left\{ \begin{matrix} \text{all the matrices obtained by permuting} \\ \text{the columns of } \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix} \end{matrix} \right\}.$$

The user’s slides are constructed by the same method as described in subsection 3.1. To construct a display image, all columns of the matrix group I correspond to a query image1 which is revealed by stacking all the slides of the user to the display image. Each column of the matrix group II alternately corresponds to query images 1 and 2 which are revealed by stacking each slide to one. For each query image, if it is a white (W) pixel, the column corresponding to the query image must contain an even number of 1’s and if it is a black (B) pixel, an odd number of 1’s. To achieve these goals, we choose ‘0’ or ‘1’. Table 2 shows a construction example of the row vector to generate the display image for the case of $n=3$.

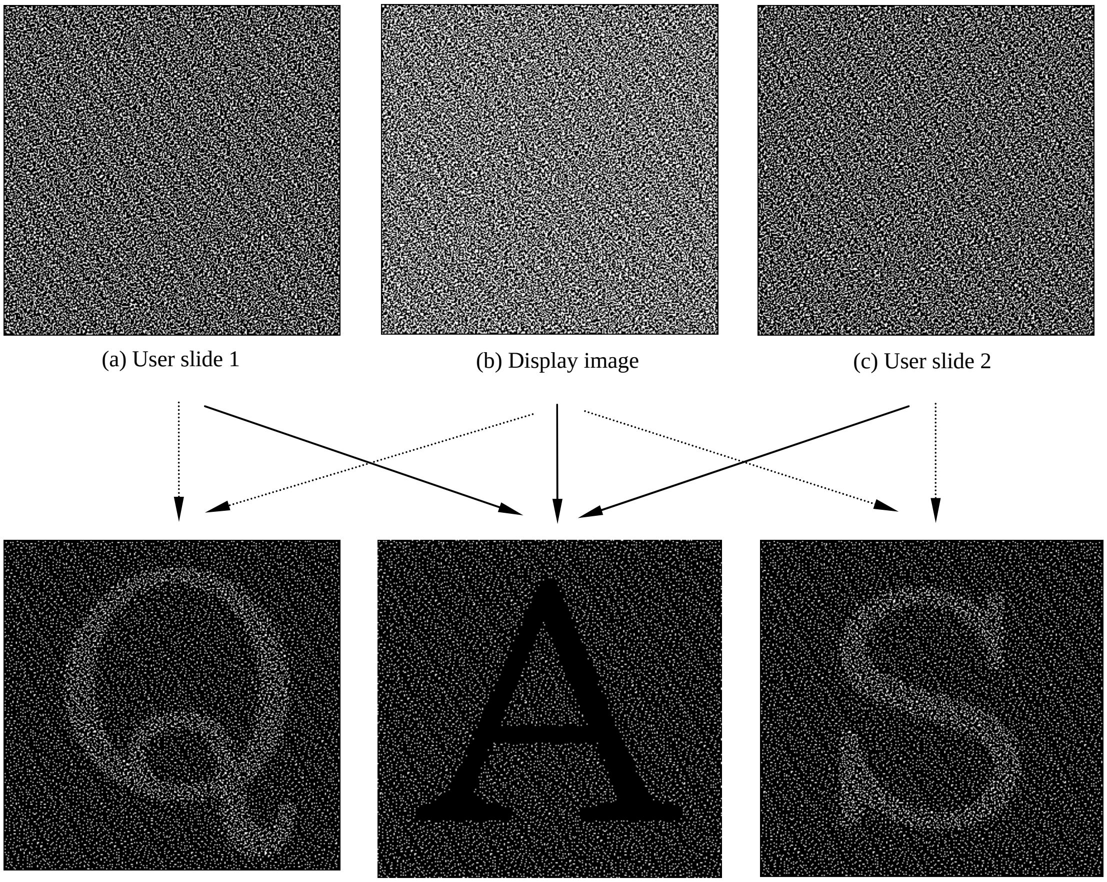
When stacking a slide to the display (generating images 2 and 3), the Hamming weight of a share for white is $2^{n-1}+2n-3$ and the Hamming weight for black is $2^{n-1}+2n-4$. Also, when stacking all slides to the display(generating query image 1), the Hamming weight for white is $2^{n-1}+2n-3$, the Hamming weight for black is $2^{n-1}+2n-2$. Fig. 2 shows the result of the proposed method for $n=3$. Fig. 2. (d) and (f) are revealed in reversion because the Hamming weight for white is larger than that for black. And (e) (stacking all user slides on the displayed image) can reveal the third secret image.

4. Conclusion

We have proposed a generalized construction method concealing several query images in a display image. Furthermore, we have proposed a new construction method based on Droste’s technique. The new method makes it possible to reveal a different query image by stacking a user's slides on a displayed image.

[References]

1. T.Matsumoto, H.Imai, “Human Identification Through Insecure Channel”, Advanced in Cryptology-EUROCRYPT’91, pp.409-421, 1991.
2. M.Naor and A.Shamir, “Visual Cryptography”, Advanced in Cryptoloy-EUROCRYPT’94, pp1-12, May 1994.
3. T.Katoh and H.Imai, “An Application of Visual Secret Sharing Scheme Concealing Plural Secret Images to Human Identification Scheme”, Proc. of SITA’96, pp.661-664, December 1996(in Japanese).
4. S.Droste, “New Results on Visual Cryptography”, Advanced in Cryptology-CRYPT’96, pp.401-415, Aug. 1996.



(a) User slide 1

(b) Display image

(c) User slide 2

(d) User side 1 + Display image

(e) All slides + Display image

(f) User slide 2 + Display image

Fig.2 Decryption of Secret Images in the Proposed Method