Extended Visual Cryptography for Natural Images

Conference Paper *in* Journal of WSCG · January 2002

Source: DBLP

CITATIONS
172

READS
984

2 authors, including:

Yasushi Yamaguchi
The University of Tokyo
83 PUBLICATIONS **905** CITATIONS

SEE PROFILE

EXTENDED VISUAL CRYPTOGRAPHY FOR NATURAL IMAGES

Mizuho NAKAJIMA

Yasushi YAMAGUCHI

Department of Graphics and Computer Sciences
Graduate School of Arts and Sciences
The University of Tokyo
3-8-1 Komaba, Meguro-ku, Tokyo 153-8902, Japan
{mitzy, yama}@graco.c.u-tokyo.ac.jp

ABSTRACT

Extended Visual Cryptography[Ateni01] is a type of cryptography which encodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is done directly by the human visual system with no special cryptographic calculations. This paper presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. While the previous researches basically handle only binary images, this paper establishes the extended visual cryptography scheme suitable for natural images. Generally, visual cryptography suffers from the deterioration of the image quality. This paper also describes the method to improve the quality of the output images. The trade-off between the image quality and the security are discussed and assessed by observing the actual results of this method. Furthermore, the optimization of the image quality is discussed.

Keywords: Visual Cryptography, Halftoning, Extended Visual Cryptography

1 INTRODUCTION

Visual cryptography[Naor95] is a kind of cryptography that can be decoded directly by the human visual system without any special calculation for decryption. As shown in Fig.1, our visual cryptography system takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. This type of visual cryptography, which reconstructs the image by stacking some meaningful images together, is especially called *Extended Visual Cryptography*[Ateni01]. In this paper, the pictures shown on the output images are called *sheets* and the resulting image reconstructed by stacking the two sheets together is called the *target*.

Previous works on the extended visual cryptography deal with binary images such as text images, but natural images such as photographs are difficult to handle in such scheme. This paper establishes the extended visual cryptography scheme for natural images. Generally, visual cryptography suffers from the deterioration of the image quality. This paper also describes the method to improve the quality of the output image.

Section 2 gives an overview of the visual cryptography. In Section 3, this paper explains a fundamental theory and the process to implement the extended visual cryptography. Section 4 discusses a way to improve image quality, as well as the trade-off between the image quality and the security of the cryptography. In Section 5, discussions are made on future works such as color scheme and more flexible combination of the sheets and the target. Finally, the concluding remarks are made in Section 6.

2 VISUAL CRYPTOGRAPHY

2.1 Visual Secret Sharing Scheme

The basic model of the visual cryptography consists of a several number of transparency sheets.

On each transparency a ciphertext is printed which is indistinguishable from random noise. The hidden message is reconstructed by stacking a certain number of the transparencies and viewing them. The system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations.
Naor and Shamir have developed *the Visual Secret Sharing Scheme(VSSS)* to implement this model[Naor95]. In k out of n VSSS(which is also called $(k,\ n)$ scheme), an binary image(picture or text) is transformed into n sheets of transparencies of random images. The original image becomes visible when any k sheets of the n transparencies are put together, but any combination of less than k sheets cannot reveal the original binary image.
In the scheme, one pixel of the original image is reproduced by m subpixels on the sheets. The pixel is considered "on"(transparent) if the number of transparent subpixels is more than a constant threshold, and "off" if the transparent subpixels is less than a constant lower threshhold, when the sheets are stacked together. The contrast α is the difference between the on and off threshhold number of transparent pixels.
Ateniese et al. has extended the (k, n) VSSS to general access structures where senders can specify all qualified and forbidden subsets of n participants[Ateni96]. Droste considered the problem of sharing more than one secret images among a set of participants, and proposed a method to reconstruct different images with different combinations of sheets[S.Dro96]. Hofmeister has discussed to maximize the contrast α using linear programing in the cases of $k \in \{3,\ 4,\ n\}$[Hofme97].

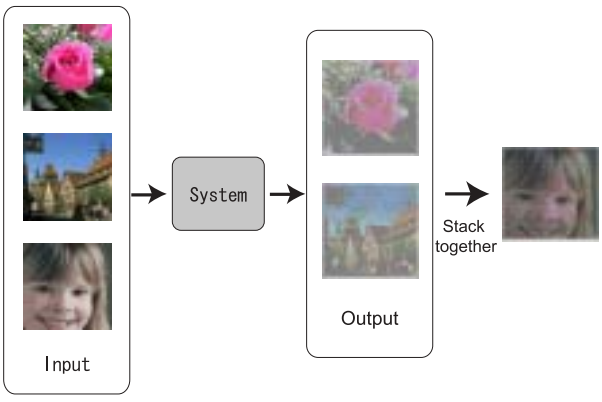

Figure 1: The basic idea of the proposed system.

2.2 Extended Visual Cryptography

Naor and Shamir have mentioned an extention of the model which conceals the very existence of the secret message[Naor95]. That is, each sheet carries some meaningful images rather than random dots. They refered to the (2, 2) example with the number of subpixels $m = 4$.
Ateniese has formalized this framework as *the Extended Visual Cryptography* and developed a scheme for general access structures[Ateni01]. They also discuss the trade-off between the contrast of the each images on the sheets and that of the resulting image when stacked together in $(k,\ k)$ cases.

2.3 Application to the Grayscale and Color Images

A few researches have discussed the visual cryptography for grayscale and color images. Naor and Shamir mentioned the extention of their scheme to grayscale images[Naor95]. That is, to represent the graylevels of the hidden image by controlling the way how the opaque subpixels of the sheets are stacked together. The grayscale version of the visual cryptography is fundamentally proposed in the paper.
There are some researches that deal with color images[Naor96, Koga98, E.R.V97, Rijme96]. Naor and Shamir discussed the visual cryptography scheme which reconstructs a message with two colors, by arranging the colored or transparent subpixels[Naor96]. Koga et al. devised a lattice-based $(k,\ n)$ scheme[Koga98]. The approach by Verheul and van Tilborg[E.R.V97] is basically similar to Koga's. Both approaches assign a color to a subpixel at a certain position, which means that displaying m colors uses $m-1$ subpixels. The resulting pixels contain one colored subpixel and the rest of the subpixels are black. Therefore the more colors are used, the worse the contrast of the images becomes significantly. Their approaches cannot be applied to the extended visual cryptography, either. Rijmen and Preneel talked about enabling multicolors with relatively less subpixels(24 colors with $m = 4$)[Rijme96]. However each sheets must contain color random images, which means applying this approach to the extended visual cryptography is impossible.
This paper focuses on the (2, 2) scheme and discusses the method to deal with the natural images with intermediate graylevels. It also shows how to enhance the contrast.

3 EXTENDED VISUAL CRYPTOGRAPHY FOR NATURAL IMAGES

3.1 Fundamentals of Extended Visual Cryptography

Visual cryptography is based on Boolean operations. Therefore halftoning is necessary for applying visual cryptograpy to grayscale images. This section makes some consideration on the average transparency of a pixel in the context of halftoning techniques. Let Ω represent the entire region of a pixel, and $t(\mathbf{x})$ to be the transparency of a point $\mathbf{x}$ within the region.
Taking the human visual system into account, the average transparency t_Ω becomes

$$t_\Omega = \frac{\int_\Omega t(\mathbf{x})dA}{A_\Omega},$$

where $A_\Omega = \int_\Omega dA$ denotes the area of Ω.
The average transparency of the target pixel is as follows. Let $t_1(\mathbf{x})$ and $t_2(\mathbf{x})$ to be the transparencies of sheet 1 and sheet 2, respectively, at the point $\mathbf{x}$. The target pixel's transparency at $\mathbf{x}$, achieved by placing the two sheets together, is $t_1(\mathbf{x})\cdot t_2(\mathbf{x})$, and thus the average transparency of the target for the region Ω becomes $t_T = \frac{\int_\Omega t_1(\mathbf{x})\cdot t_2(\mathbf{x})dA}{A_\Omega}$.
For usual grayscale images, transparencies are constant within a pixel region, $t_T = t_1 \cdot t_2$. In contrast, for halftoned binary images, the tranparency of every point is $t(\mathbf{x}) \in \{0, 1\}$. The average transparency becomes:

$$t_\Omega = \frac{A_T}{A_\Omega},$$

where $A_T = \int_\Omega t(\mathbf{x})dA$ denotes area of transparent$(t(\mathbf{x}) = 1)$ region in Ω.
The stacking-together operation of the binary images is represented by the Boolean product of the transparencies $t_T = \frac{A_{12}}{A_\Omega}$, where A_{12} denotes the area with $t_1(\mathbf{x}) = 1$ and $t_2(\mathbf{x}) = 1$. The range of A_{12} is

$$A_{12} \in [\max(0, (A_1 + A_2) - A_\Omega), \min(A_1, A_2)]$$

as shown in Fig.2. Here notion [ ] denotes intervals and $[a,\ b] = \{x | a \le x \le b\}$. Therefore the range of t_T is

$$t_T \in [\max(0, t_1 + t_2 - 1), \min(t_1, t_2)], \quad (1)$$

where t_1 and t_2 denote the transparencies of the entire pixel region for sheet 1 and 2, respectively, and $t_1 = \frac{A_1}{A_\Omega},\ t_2 = \frac{A_2}{A_\Omega}$. The principals of the extended visual cryptography lie in controlling the transparency of the target by arranging the transparent subpixels of each sheet.
In this paper, the range of the transparency in an entire image is called a dynamic range of the image. Suppose the dynamic ranges of the two sheets are the same and they are $t_1, t_2 \in [L, U] \subseteq [0, 1]$. If the dynamic range of the target fulfills :

$$t_T \in [\max(0, 2U - 1), L], \quad (2)$$

then any *triplet* (a set of two sheet-pixels and one target-pixel of the same position) satisfies the condition (1). Therefore the condition (2) is sufficient to the perfectly secure extended visual cryptography. Any three images can be processed once their contrasts are reduced so that they satisfy the condition (2).
As discussed in the previous section, former researches on extended visual cryptography deal with binary original images, and because of this, only the condition (2) is presented as the encryption restriction, and is generally called "the constraint of the dynamic range." Further discussion on the issue of conditions will be made in Section 4.1.

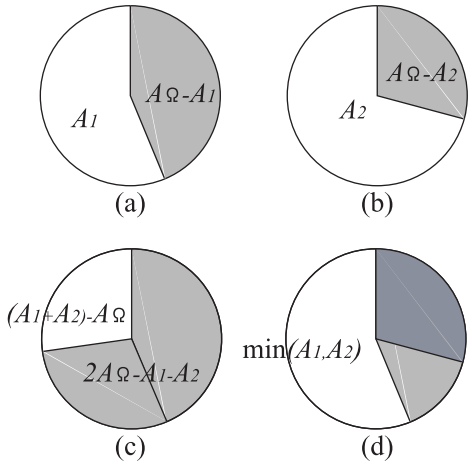

Figure 2: The range of area of the target pixel's transparent region. A_1(see (a)) denotes the transparent area in sheet 1 and A_2(see (b)) denotes that of sheet 2. At (c), the transparent area achieved by stacking the two sheets is minimum. The area is maximum at (d).

3.2 The Process

There are a variety of halftoning techniques. A non-periodic and dot-dispersed dithering algorithm is most suitable for our approach since it allows arbitrary subpixel arrangements[Gomes97]. Therefore the error-diffusion algorithm[Floyd75] has been adopted.
The encryption process consists of determining the arrangements of transparent subpixels on each sheet according to the pixel transparencies, $t_1,\ t_2$ and t_T, as shown in Fig.3. Here, one pixel in a grayscale image is halftoned by m subpixels. Encryption is applied to three quantized images,

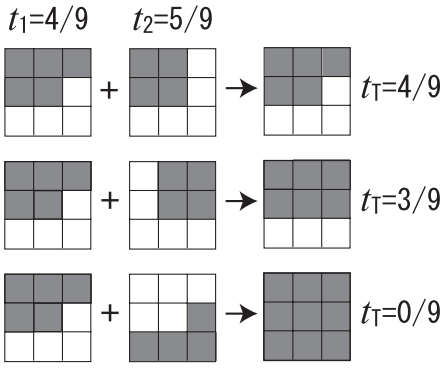

Figure 3: Two examples of subpixel arrangements. With $t_1 = \frac{4}{9}$ and $t_2 = \frac{5}{9}$, $t_T = \frac{4}{9}$ can be achieved by arranging the subpixels as the top example. Also, arranging them as the middle and bottom examples makes $t_T = \frac{3}{9}$ and $t_T = \frac{0}{9}$, subsequently.

pixel by pixel. Let s_1, s_2 and s_T denote the number of transparent subpixels in the pixels of sheet1, sheet2 and target, respectively. The pixel transparencies of the sheets and the target become $t_1 = \frac{s_1}{m}, t_2 = \frac{s_2}{m}$ and $t_T = \frac{s_T}{m}$, respectively. Here we assume the triplets are subject to the condition (2), i.e., $s_1,\ s_2 \in \{l,\ \cdots,\ u\}$ and $s_T \in \{\max(0, \frac{2u-m}{m}),\ \cdots,\ \frac{l}{m}\}$.
Encryption is a task of randomly choosing a matrix S from a set of $2 \times m$ Boolean matrices $C^{t_1,t_2}_{t_T}$, according to the number of transparent subpixels, s_1, s_2 and s_T. For instance, in the the upper example of Fig.3, Boolean matrix S is $\begin{bmatrix} 0&0&0&0&0&1&1&1&1 \\ 1&0&0&1&0&0&1&1&1 \end{bmatrix}$.
The set of Boolean matrices $C^{t_1,t_2}_{t_T}$is computed from s_1, s_2, s_T and m as follows. Consider m sets of sheet1, sheet2 and target subpixels, and let $\tau_1, \tau_2, \tau_T \in \{0,\ 1\}$ denote the transparencies of each subpixels. Here 0 means 100% opaque(i.e., no light transmission) and 1 means 100% transparent (i.e., transmits all light).
As discussed in Section 3.1, transparency of the target subpixels τ_T is given by Boolean product of the transparencies of the sheet subpixels, τ_1 and τ_2. Therefore the m sets of subpixels can be categorized into four subsets, and let $P_{\tau_1\tau_2}$ denote the cardinalities of the each subsets. Thus, the number of subpixel pairs with which both sheet1 and sheet 2 subpixels are transparent is P_{11}, the number of the pairs with sheet 1 transparent and sheet 2 opaque is P_{10}. In the same way, P_{01} denotes the number of the pairs with sheet1 opaque and sheet2 transparent, and P_{00} denotes the number of both opaque ones. They are shown in Table.1.

There exist following relationships among

Table 1: The transparencies of the subpixels τ_1, τ_2 and τ_T, and the number of each pairs.

subpixel transparency			number of
τ_1	τ_2	τ_T	subpixel pairs
1	1	1	P_{11}
1	0	0	P_{10}
0	1	0	P_{01}
0	0	0	P_{00}

$P_{\tau_1\tau_2},\ m,\ s_1,\ s_2$ and s_T

$$\begin{aligned} s_1 &= P_{11} + P_{10}, \\ s_2 &= P_{11} + P_{01}, \\ s_T &= P_{11}, \\ m &= P_{11} + P_{01} + P_{10} + P_{00}. \end{aligned}$$

The sufficient condition (2) guarantees every $P_{\tau_1\tau_2}$ is non-negative.
The set $C^{t_1,t_2}_{t_T}$ consists of the matrices which have P_{11} columns of $[1\ 1]^{\mathbf{T}}$, P_{10} columns of $[1\ 0]^{\mathbf{T}}$, P_{01} columns of $[0\ 1]^{\mathbf{T}}$ and P_{00} columns of $[0\ 0]^{\mathbf{T}}$.

The arrangement of m subpixels of each sheet is determined by arbitrarily selecting the matrix S from $C^{t_1,t_2}_{t_T}$. In the case of $m = 9,\ s_1 = 4,\ s_2 = 5$ and $s_T = 3$ (the same as upper example of Fig.3), for instance, the numbers of subpixel pairs are $P_{11} = 3,\ P_{10} = 1,\ P_{01} = 2,\ P_{00} = 3$, and $C^{\frac{4}{9},\frac{5}{9}}_{\frac{3}{9}}$ becomes:

$$C^{\frac{4}{9},\frac{5}{9}}_{\frac{3}{9}} = \left\{ \begin{array}{c} \text{all permutations of} \\ \text{the columns of} \end{array} \begin{bmatrix} 1&1&1&1&0&0&0&0&0 \\ 1&1&1&0&1&1&0&0&0 \end{bmatrix} \right\}.$$

4 IMPROVING THE IMAGE QUALITY

4.1 The Contrast Enhancement

This paper aims at natural images, eg.,grayscale images, with higher image quality. This section discusses the contrast enhancement as a way of improving the quality.
Firstly the proposed method applies affine transformation to the each pixel's intensity (transparency) in order to reduce the contrast of the input images, but not as far as the condition (2), since though contrast can be enhanced, it is difficult to encrypt the input images themselves, as we discuss later.
For simplicity, suppose that the contrast of the sheets and that of the target are the same fixed value K. It is obvious that 0 is the most appropriate value for the lower bound of the target because the target must be darker than both

sheets. Let L denote the lower bound of the sheet dynamic range. Therefore, the resulting dynamic ranges of the sheets and the target are $t_1, t_2 \in [L, L+K] \subseteq [0,1]$ and $t_T \in [0, K] \subseteq [0,1]$, respectively.

When enhancing the contrast, it is necessary to consider the condition for the encryption. The condition (2) is sufficient for encryption with any three arbitrary images. In fact, the encryption can be performed if, in each triplet (pixels of two sheets and the target), the condition (1) is satisfied, which is a looser condition than the condition (2). In case of natural images, most triplets satisfy condition (1) even if the three images violate the condition (2).

For binary images, the conflicts are fatal to the encryption. However, grayscale images can tolerate those conflicts by adjusting graylevels of the conflicting triplets. The proposing method performs both halftoning and encryption process simultaneously to enable this adjustment with natural results. As the contrast enhances, the conflicts with the condition (1) are adjusted and the resulting errors are diffused to the nearby pixels.

Consider a three-dimentional space with pixel transparencies of sheet1, sheet2 and target, t_1, t_2 and t_T, as its axes. A pixel triplet corresponds to a point in this space. After the affine transformation, all the triplets lie inside the cube K on a side shown in Fig.4. Any triplets in the region shadowed in gray as in Fig.4 satisfy the condition (1). Let $\mathbf{p} = (t_1,\ t_2,\ t_T)$ denote pixel transparencies of a triplet before the quantization, and $\bar{\mathbf{p}} = (\bar{t}_1,\ \bar{t}_2,\ \bar{t}_T)$ to be its quantized values. When $\bar{t}_1, \bar{t}_2$ and $\bar{t}_T$ violate the condition (1) the point $\bar{\mathbf{p}}$ lies outside of the region in Fig.4, so $\bar{\mathbf{p}}$ is moved to a grid-point within the region $\mathbf{p}' = (t'_1,\ t'_2,\ t'_T)$, whose distance to $\mathbf{p}$ is minimum. The quantization error of the point becomes $\mathbf{p}' - \mathbf{p}$.

Therefore, when the triplet violates the condition (1), the errors to be diffused using error-diffusion algorithm are

$$\delta_1 = t'_1 - t_1, \quad \delta_2 = t'_2 - t_2, \quad \delta_T = t'_T - t_T,$$

for sheet 1, sheet 2 and target, respectively. Thus extending the concept of quantization error relaxes the restriction on the dynamic range of the entire images, i.e., the condition (2), and enables natural encryption.

4.2 Considerations on Security

The constraint of the dynamic range is relaxed by diffusing the amount of conflict as a part of quantization error. High frequency of the conflict, however, may spoil the result because the information from the sheets and the target interact with each other. This causes a security issue that

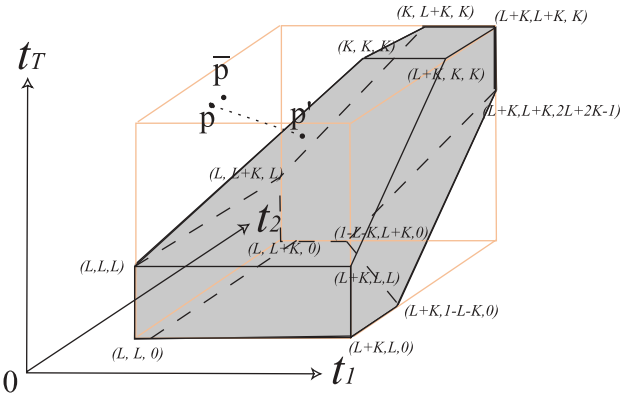

Figure 4: the range that satisfy the condition (1).

is target information appearing on the sheets. In other words, the proposing extended visual cryptography scheme is not perfectly secure.

Let us consider that a picture generated by dissolving multiple images is given. It is fundamentally impossible to retrieve original images from the given one. However, the human high-level visual system retains an ability to separate the originals from the given image. Therefore the security of the visual cryptography must be considered with the human perception, and its assessment can be done only by actually viewing the resulting output images. Several experiments are performed on the trade-off between contrast enhancement and the security of the images.

Constraint fulfillment rate(CFR) is defined as the ratio of triplets which satisfy the condition (1) out of the whole triplets of the entire images. In the experiments, various ciphersheets are created with different contrasts, and their CFR and the image qualities are observed(Fig.6 and Fig.7). It was found that when the CFR is below 0.6, the error influence becomes too loud that is the target picture becomes perceivable from the sheets.

4.3 Determining the Lower Bound of the Dynamic Ranges

By the method discussed in Section 4.1, the dynamic range can be enhanced beyond the condition (2). As discussed, the dynamic ranges of sheets and target are $t_1, t_2 \in [L, L+K] \subseteq [0,1]$ and $t_T \in [0, K] \subseteq [0,1]$, respectively. Given K, the lower bound of the sheet dynamic ranges L is remained to be the free parameter. It should be possible to increase the CFR and to improve the image quality by setting L to the appropriate value. This section discusses a method to calculate L which maximizes the CFR for a given contrast K.

Assume that the distribution of the transparency is stocastic in the images. Let $p_1(t_1)$, $p_2(t_2)$ and $p_T(t_T)$to be the probability density functions of the transparencies t_1, t_2 and t_T, respectively. The CFR P, which is the possibility that t_1, t_2 and t_T satisfy the condition (1) is given by the folowing equation:

$$P(K,L) = \int\int\int_D p_T(t_T)\, p_1(t_1)\, p_2(t_2)\, dt_1\, dt_2\, dt_T$$

Here, D denotes the region shown in Fig.4 which satisfies the constraint.
From Fig.4, it is obvious that D is determined by K and L, which means that P is a function of K and L. The upper graph of Fig.5 shows the theoretical CFR $P(K,L)$ with the assumption that transparencies are evenly distributed in all two sheets and the target. It is the relative value of D to the cube K on a side.

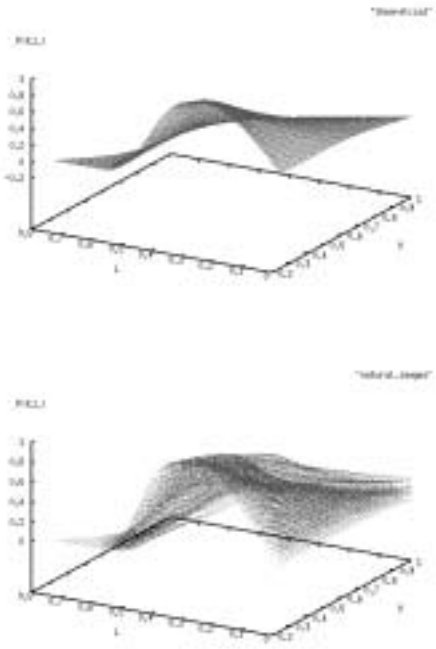

Figure 5: The relationship among K, L and $P(K,L)$. Above: theoritical values. Below: measured values from the actual results.

Experiments are performed by providing nine different patterns of the three input images and changing K and L by $\frac{1}{100}$ in the range of $\frac{1}{4} \leq K \leq 1$, $0 \leq L \leq K$, and $K + L \leq 1$. This is shown in the lower graph of Fig.5. It is observed from the graph that the CFR values are rather perturbed in the actual case. However, the tendency of the CFR in terms of K and L is basically the same in theory and in the actual values.
Therefore it concludes that the theoretical CFR $P(K,\ L)$ shown in Fig.5 above, which was obtained by assuming even distribution of the transparencies, is effective for maximizing the CFR.

5 FUTURE WORKS

Here we discuss two natural extentions to the presented schemes. That is, the scheme for colored images and more flexible combination of sheets and the resulting targets.
There is a straightfoward way to extend this scheme to color images. Generally in printing, color images can be separated into channels of three primary colors, i.e., cyan, magenta and yellow, and each channel can be treated as an independent grayscale image. In a very naive approach, the system applies the encryption to each channel and merges the result to get the colored output. Under the ideal subtractive color mixing model, stacking the two colored sheets reveals the colored target[1]. In reality, however, such ideal subtractive color mixture is unlikely due to the properties of ink, transparencies, etc. It needs to establish a sophisticated color mixing model for the extended visual cryptography with better color quality.
Another natural extention isto allow flexible combination of sheets and the target images. The scheme this paper has discussed is restricted to the combination of three images, two for the sheets and one for the target, which is reconstructed by stacking the two sheets together. However, extending the discussion in Section 4.1 can realize any combination of sheets and targets by solving quadratic optimization problems.

6 CONCLUSION

This paper proposed the extended visual crypography scheme for natural images. Next it showed a method to improve the image quality of the output by enhancing the image contrast beyond the constraints given by the previous studies. The method enables the contrast enhancement by extending the concept of error and by performing halftoning and encryption simultaneously. The trade-off between the image quality and the security are assessed by observing the actual results of this method. Furthermore, the optimization of the image quality at a given contrast is discussed. Under an assumption that the occurence of the violations is stochastically even in the images, a CFR function is introduced for the image quality optimization. The validity of the assumption and the effect of image quality improvement are also

[1]The simulated result can be found in the proceedings CDROM.

verified with the experiments. Fig.6 shows an example of the results created by proposed method.

Figure 6: The resulting output of the extended visual cryptography scheme using the proposed method. Top and middle figure are the two sheets, and the result of stacking them together(target) is shown at the bottom: the number of subpixels $m = 16$, the contrast $K = 0.688$, and the CFR $= 0.702$.

REFERENCES

[Ateni96] G. Ateniese, C. Blundo, A. de Santis, and D. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129(2):86–106, 1996.

[Ateni01] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250:143–161, 2001.

[E.R.V97] E.R.Verheul and H.C.A.van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. *Design Codes and Cryptography*, 11(2):179–196, 1997.

[Floyd75] R.W. Floyd and L. Steinberg. An adaptive algorithm for spatial greyscale. *Proc.SID*, 17/2:75–77, 1975.

[Gomes97] Jonas Gomes and Luiz Velho. *Image Processing for Computer Graphics*. Springer, 1997.

[Hofme97] T. Hofmeister, M. Krause, and H.U.Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. In *COCCON '97, Lecture Notes in Computer Science*, volume 1276, pages 176–185, Berlin, 1997. Springer.

[Koga98] Hiroki Koga and Hirosuke Yamamoto. Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. *IEICE Transaction on Fundamentals*, E81-A(6):1262–1269, June 1998.

[Naor95] M. Naor and A. Shamir. Visual cryptography, advances in cryptology. *Eurocrypt '94 Proceeding LNCS*, 950:1–12, 1995.

[Naor96] M. Naor and A. Shamir. Visual cryptography ii: Improving the contrast via the cover base. *Theory of Cryptography Library*, (96-07), 1996.

[Rijme96] V. Rijmen and B. Preneel. Efficient colour visual encryption or shared colors of benetton. presented at EUROCRYPT'96 Rump Session, available as `http://www.iacr.org/conferences/ec96/rump/preneel.ps`, 1996.

Figure 7: Output sheets with different CFRs. These sheets are created using the same combination of the input images as Fig.6. From top to bottom, the CFRs are 0.617, 0.567 and 0.505 accordingly. The contrasts are 0.75, 0.567 and 0.875, respectively. In either cases, number of subpixels m is 16.

[S.Dro96] S.Droste. New results on visual cryptography. In *Advances in Cryptology – CRYPTO'96*, pages 401–415. Springer, 1996.