Tracking-Tolerant Visual Cryptography

Ruofei Du*, Eric Lee†, and Amitabh Varshney‡ *Fellow, IEEE*
Augmentarium, Department of Computer Science, and University of Maryland Institute for Advanced Computer Studies
University of Maryland, College Park

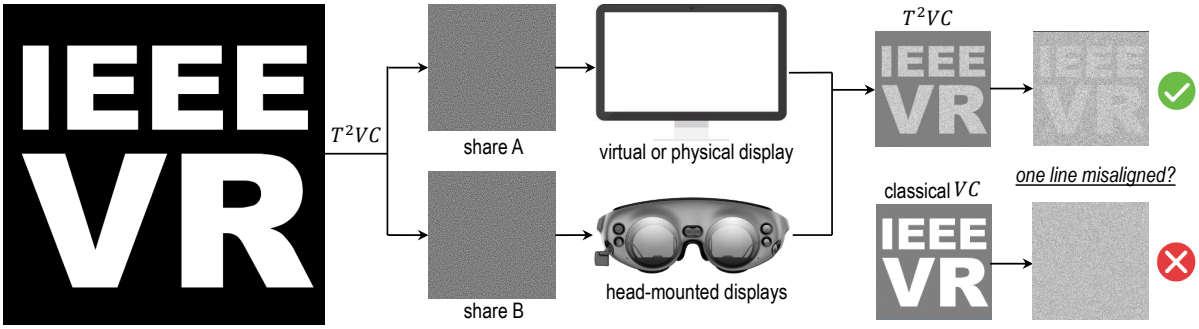


Figure 1: Results and overview of our system, T^2VC, which is able to split a confidential message into two shares of images and guarantees that the original information could not be revealed with either share of image alone. When the user looks through the two aligned images in the head-mounted display, the secret message is revealed directly to the user's human visual system. Nevertheless, head jittering may cause the two images to slightly misalign with each other even with visual tracking algorithms. Our algorithm outperforms the classic visual cryptography algorithm in presence of one or two rows of misalignment.

Abstract

We introduce a novel secure display system, which uses visual cryptography [4] with tolerance for tracking. Our system brings cryptographic privacy from text to virtual worlds [3]. Much like traditional encryption that uses a public key and a private key, our system uses two images that are both necessary for visual decryption of the data. The public image could be widely shared on a printed page, on a traditional display (desktop, tablet, or smartphone), or in a multi-participant virtual world, while the other private image can be exclusively on a user's personal AR or VR display. Only the recipient is able to visually decrypt the data by fusing both images. In contrast to prior art, our system is able to provide tracking tolerance, making it more practically usable in modern VR and AR systems. We model the probability of misalignment caused by head or body jitter as a Gaussian distribution. Our algorithm diffuses the second image using the normalized probabilities, thus enabling the visual cryptography to be tolerant of alignment errors due to tracking.

Keywords: visual cryptography, augmented reality (AR), tracking

Index Terms: H.5.1 [Information Interfaces and Presentation (e.g., HCI)]: Multimedia Information Systems—Artificial, augmented, and virtual realities I.3.3 [Computer Graphics]: Picture/Image Generation—Display algorithms

1 Introduction

We present T^2VC, a tracking-tolerant visual cryptography system for AR or VR head-mounted displays (HMDs). Our system presents a practical and robust cryptographic solution that eliminates every device from the trusted computing bases (TCB) and assumes no connection between the TCBs. First, T^2VC splits the confidential information (as an image) into two shares. One share of data is displayed on the ordinary screen while the other share of data is displayed on the HMD. The user decrypts the message by visually aligning the two shares of information. Our work is built upon the pioneering research by Andrabi *et al.* [1], which first demonstrates the potential of using AR HMD to reveal secret messages using the visual cryptography system induced by Naor and Shamir [4]. However, their system requires a chinrest and takes over ten seconds for the users to recognize a single character. This is largely due to head jitters when manually aligning the two images.

To solve the challenge of head jittering, T^2VC leverages the visual tracking modules in *Magic Leap One*[1]. While visual tracking algorithms may roughly align two images together, they may still suffer from one or two pixels of misalignment. Our system further models the misalignment of head jitter using a 2D Gaussian distribution. We have developed a novel algorithm to enhance the visibility of the classical visual cryptography via diffusion with Gaussian kernels, thus enabling the algorithm to be tolerant with misalignment.

2 Algorithm

The main idea behind T^2VC is: for each pixel p in one share, we model the probability of misalignment on another pixel q as a 2D Gaussian distribution centered at the pixel p. In this way, we sacrifice a little contrast in the fused result for better clarity when one or two rows of misalignment occurs.

2.1 Preprocessing

Following [1] and [4], given a confidential visual image $\boldsymbol{I}$, we first generate a binary image $\hat{\boldsymbol{I}}$ by thesholding every 2×2 block of pixels in $\boldsymbol{I}$. Here, we denote $\mathscr{F}(\hat{\boldsymbol{I}})$ and $\mathscr{B}(\hat{\boldsymbol{I}})$ as the set of foreground (white) and background (black) pixels of $\hat{\boldsymbol{I}}$, respectively.

Next, we model the range of misalignment as an $s\times s$ square and generate an $s\times s$ 2D Gaussian kernel $\mathscr{G}(x,y,\sigma)$ at scale σ:

$$\mathscr{G}(x,y,\sigma)=\frac{1}{2\pi\sigma^2}e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{1}$$

In our experiments, we choose $s=3,\sigma=1.0$ and $s=5,\sigma=2.0$.

*e-mail: me@duruofei.com, now at Google LLC, San Francisco.
†e-mail: ericlee@umiacs.umd.edu
‡e-mail: varshney@cs.umd.edu

[1]Magic Leap One: `https://magicleap.com/magic-leap-one`

ALGORITHM 1: Tracking-Tolerant Visual Cryptography

Input: a binary secret image $\hat{\boldsymbol{I}}$
Output: two shares of information $\boldsymbol{I}^{\alpha}$ and $\boldsymbol{I}^{\beta}$
Generate a random share of $\boldsymbol{I}^{\alpha}$;
for *each* 2×2 *block* b_{rc} *of* $\hat{\boldsymbol{I}}$ **do**
  for *each* 2×2 *block* b_{ij} *of* $\hat{\boldsymbol{I}}$, *where* $|r-i|\leq\frac{s}{2},|c-j|\leq\frac{s}{2}$ **do**
    if $b_{ij}\in\mathscr{F}(IB)$ *or AllowBackgroundDiffusion* **then**
      Look up the probability of misaligning b_{rc} with b_{ij} from the from the Gaussian kernel $\mathscr{G}(x,y,\sigma)$: $\mathscr{P}(b_{rc},b_{ij})\leftarrow\mathscr{G}(r-i,c-j,\sigma)$;
      Increase the normalization factor of b_{rc}: $\mathscr{N}_{rc}\leftarrow\mathscr{N}_{rc}+\mathscr{P}(b_{rc},b_{ij})$;
    end
  end
  Normalize probabilities: $\mathscr{P}(b_{rc},b_{ij})\leftarrow\mathscr{P}(b_{rc},b_{ij})/\mathscr{N}_{rc}$;
  Generate a random uniform sample: $r\in[0,1]$;
  Set the accumulated probabilities: $\mathscr{A}_{rc}\leftarrow 0$
  for *each* 2×2 *block* b_{ij} *of* $\hat{\boldsymbol{I}}$, *where* $|r-i|\leq\frac{s}{2},|c-j|\leq\frac{s}{2}$ **do**
    if $b_{ij}\in\mathscr{F}(IB)$ *or AllowBackgroundDiffusion* **then**
      $\mathscr{A}_{rc}\leftarrow\mathscr{A}_{rc}+\mathscr{P}(b_{rc},b_{ij})$;
      if $r\leq\mathscr{A}_{rc}$ **then**
        $(p,q)\leftarrow(i,j)$ **break**;
      end
    end
  end
  $\boldsymbol{I}^{\beta}_{rc}\leftarrow b_{pq}\in\mathscr{B}(\hat{\boldsymbol{I}})\ ?\ \boldsymbol{I}^{\alpha}_{pq}\ :\ WHITE-\boldsymbol{I}^{\alpha}_{pq}$;
end

2.2 Generation of Two Shares

T^2VC generates the first share as the classical VC approach. For each 2×2 block of pixels in the first share, we randomly choose one of the six VC patterns. Next, we carry out two solutions to deal with the possible misalignment: 1) T^2VC^*: for the second share, we only diffuse the foreground pixels: each foreground pixel has a probability to be misaligned with one of its surrounding pixels; in this way, when the two shares match perfectly, the background is unchanged, but the foreground becomes darker. 2) T^2VC: for the second share, we diffuse both the background and foreground pixels to enhance the contrast: every pixel has a probability to be misaligned with one of its surrounding pixels. Please refer to the source code is provided in the *supplementary material*.

3 Experimental Results

To valid the effectiveness of our algorithm, we conduct preliminary experiments via both simulation and physical deployment.

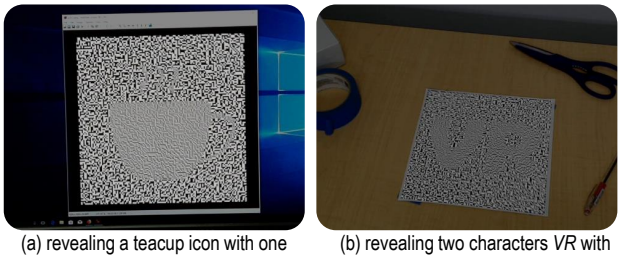
3.1 Comparison with Classical Visual Cryptography

We generate visual cryptography images at the resolution of 1024×1024 pixels using a custom C++ program using the proposed T^2VC algorithms and the classical visual cryptography algorithm under four conditions: exact match, one-row misalignment, one-column misalignment, and one-row, one-column misalignment (please refer to the supplementary material and [2] for more detail). We summarize the following insights:

1. The classical visual cryptography algorithm does not work with even a single row or column of misalignment, making it extremely challenging to interpret the image with the visual tracking being even slightly off.
2. T^2VC^* can deal with one row or one column misalignment (2 pixels) while preserving as good a contrast as the original visual cryptography algorithm. However, the contrast drops with misalignment.
3. T^2VC provides better contrast than T^2VC^* when misalignment occurs and even works with two pixels misaligned both horizontally and vertically. After increasing the size and scale of the Gaussian kernel, we can still see the secret message even with two rows (four pixels) of misalignment.

3.2 Deployment

We implement our system in Unity and deploy it on *Magic Leap One*. As shown in Fig. 2, the user can still observe the decrypted information even when the visual tracking module of Magic Leap One misaligns the two shares. In the supplementary material, we further suggest smoothly varying the brightness level of the overlaid image.



(a) revealing a teacup icon with one share displayed on a desktop monitor

(b) revealing two characters *VR* with one share printed on a piece of paper

Figure 2: Results of seeing through *Magic Leap One to* align the other share (a) in a desktop monitor, and (b) on a piece of paper.

4 Conclusion

In this paper, we have adapted visual cryptography for the current-generation AR HMDs. Our system T^2VC uses a novel visual cryptography algorithm which is tolerant to users' head jitter and slight misalignment of the two shares of encrypted visual information when visual tracking is enabled. We achieve this by modeling the misalignment through a 2D Gaussian distribution of the visual cryptography's random patterns. This allows us to trade off precise alignment with perceived contrast. As one of the first steps towards practical visual cryptography for VR and AR, we believe that our algorithm provides a versatile, commodity, off-the-shelf solution for embedding encrypted augmented reality information in the real-world displays and virtual environments [3], thereby protecting confidential data while facilitating an easy-to-use visual decryption.

Acknowledgement

This work has been supported in part by the NSF Grants 1823321, 1564212, 1429404, and the State of Maryland's MPower initiative.

References

[1] S. J. Andrabi, M. K. Reiter, and C. Sturton. Usability of Augmented Reality for Revealing Secret Messages to Users But Not Their Devices. In *11th Symposium on Usable Privacy and Security*, pp. 89–102, 2015.

[2] R. Du. *Fusing Multimedia Data Into Dynamic Virtual Environments*. PhD thesis, University of Maryland, College Park, Nov. 2018.

[3] R. Du, D. Li, and A. Varshney. Geollery: a Mixed Reality Social Media Platform. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI)*, CHI, p. 13. ACM, May. 2019. doi: 10.1145/3290605.3300915

[4] M. Naor and A. Shamir. Visual Cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 1–12. Springer, 1994. doi: 10.1109/ICRITO.2016.7784984

Supplementary Materials for Tracking-Tolerant Visual Cryptography

Ruofei Du*, Eric Lee†, and Amitabh Varshney‡ *Fellow, IEEE*
Computer Science Department and University of Maryland Institute for Advanced Computer Studies (UMIACS)
University of Maryland, College Park

1 Introduction

In this supplementary material, we introduce the background and more experimental results of T^2VC [4], a tracking-tolerant visual cryptography system. Please refer to Du *et al.* [4] for the core algorithm and contributions.

Vast amount of private data is displayed on our monitors every day. For example, the social security numbers from a company's documents or paychecks, credit card numbers shown in the bill of payment, the plain text of passwords appearing in the registration emails, as well as keycodes from the two-factor authentication messages. Nevertheless, all of these confidential data can easily be eavesdropped by skilled and persistent hackers via cyber-attacks, captured by secret video cameras, or even spied upon by any passerby. Consequently, there is an important need to have a secure mechanism for protecting information displayed on the screen.

In the past decades, researchers and scientists have designed sophisticated cryptographic algorithms to encrypt and decrypt messages. However, the device that executes the decryption algorithm could be under threat from attackers. Some other solutions incur new trusted computing base (TCB) such as smart-phones [11] and two-factor authentication [9] to address the problem. Nevertheless, the new TCB can also be compromised as a result of an implementation flaw in the secure protocol during the communication. For example, the heart-bleed bug, found in OpenSSL, a popular secure protocol, was taken advantage of to steal information over the SSL/TLS encryption [6].

The main contributions of our paper are:

- Conception and implementation of T^2VC, a secure display system which can protect confidential data against compromised operating systems and prying eyes using Magic Leap One,
- A novel algorithm to enhance the visibility of the classical visual cryptography via diffusion with Gaussian kernels, thus enabling the algorithm to be tolerant of one or two rows of misalignment,
- Tackle the problem of image stabilization and head jittering for T^2VC-like systems, which make the system practical to use.

1.1 Augmented Reality Head Mounted Displays

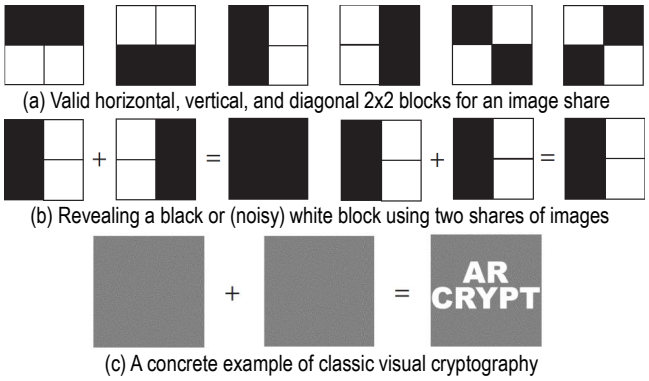
In recent years, there has been an increasing number of commercial AR head-mounted displays, such as Google Glass, ODG Smart Glasses, Meta Headsets, Epson Moverio, and Microsoft HoloLens. These displays blend the virtual information rendered by the computer with the real scene observed by the user.

There are several factors to be considered in selecting AR displays and designing rendering algorithm and content for these displays, in which field of view (FoV) and resolution are the dominant ones. In this paper, we chose Magic Leap One because it has a wider FoV and a better resolution (40° FoV, 1280×960 pixels), compared with Microsoft HoloLens (30° FoV, 1268×720 pixels), Google Glass (14° FoV, 640×360 pixels), and Epson Moverio (23° FoV, 960×540 pixels). Moreover, Magic Leap One itself is a standalone and untethered computer, which is more likely to be considered as a trusted computing base when the Internet connection is switched off.

As most of the AR headsets, Magic Leap One uses additive color mixing strategy to project visual information onto the display [10]. Consequently, for each pixel, the lower RGB values it has, the less visible it is through the display. Besides, the black color indicates total transparency in HoloLens; thus rendering a black quad through HoloLens to observe a white quad yields a white quad in the user's perception; a semi-transparent red quad through the HoloLens overlaid on a green quad yields a yellow quad.

1.2 Visual Cryptography

Visual cryptography is a cryptographic scheme which decodes a secret image without any computational cryptographic operations. The fundamental theory of visual cryptography was first presented by Naor and Shamir [12]. An example of visual cryptography with two shares is shown in Fig. 1. First, the algorithm splits one message into N shares with different transparency. Suppose the original image has $w \times w$ pixels, each share will have $\frac{w}{2} \times \frac{w}{2}$ blocks of 2×2 pixels. Each block will be one of the six patterns as shown in Fig. 1(a). Meanwhile, it ensures that a person with any K shares of the data can visually restore the image by stacking their transparencies (as in Fig. 1(b) and (c)), but any $K-1$ shares of the data cannot restore the image.



(a) Valid horizontal, vertical, and diagonal 2x2 blocks for an image share

(b) Revealing a black or (noisy) white block using two shares of images

(c) A concrete example of classic visual cryptography

Figure 1: Examples of visual cryptography proposed by Naor and Shamir [12]. (a) shows six valid patterns for one 2×2 block of pixels to be selected for an image share, (b) shows the *addition* operator when fusing one share with the other share, and (c) shows our example of revealing the characters "AR CRYPT" from two image shares.

Carlo *et al.* [2] advanced the theoretical foundations of visual cryptography for use with grey-scale images. Zhou *et al.* [13] have combined dithering techniques with visual cryptography to encrypt gray-scale images. Hou *et al.* [7] have presented novel algorithms of visual cryptography for color images. Bin *et al.* [8] have proposed

*e-mail: me@duruofei.com, now at Google LLC, San Francisco.
†e-mail: ericlee@umiacs.umd.edu
‡e-mail: varshney@umiacs.umd.edu

an edge-preserving technique for dithering to improve visual quality for visual cryptography.

Recently, Andrabi *et al.* [1] conducted the first formal user study to investigate the feasibility and usability of using Google Glass and Epson Moverio for reading visual cryptography (Fig. 2). Their system requires users to use a chin rest to minimize head jittering effects. Even with the chin rest, users spent a considerable amount of time initially aligning the image shares: ranging from 18.49 to 313.32 seconds. Apart from the effort in initial alignment, the participants spent approximately 8 seconds to decode and recognize a single plain-text character.

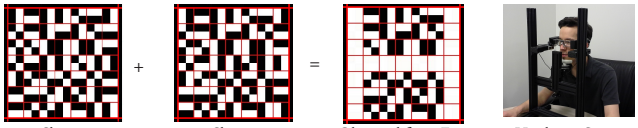
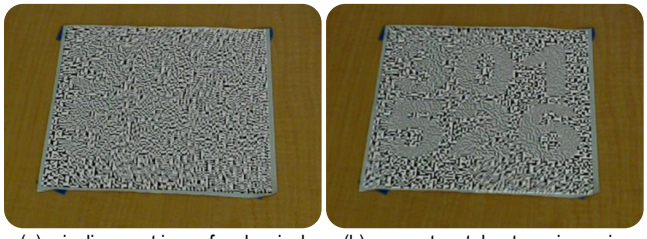


Figure 2: The pioneering AR-based visual cryptography system, developed by Andrabi *et al.* [1], is able to encrypt a single character with the help of a chin rest.

Our work is motivated by the challenge of misalignment, inspired by the study conducted by Andrabi *et al.* [1]. Specifically, we desire to enable the user to see the fused image even though the two images may not be perfectly aligned. While the state-of-the-art visual tracking algorithm has the capability of registering and stabilizing the overlaid image, it is likely that the image could move a couple of pixels with a small amount of user head jitter. An example taken from Magic Leap One's Capture Service is shown in Fig. 3



(a) misalignment issue for classical VC, even with visual tracking modules

(b) our system tolerates minor misalignment and reveals *301 526*.

Figure 3: (a) A real case of misalignment challenge for classical visual cryptography using augmented reality headsets. As long as a single line is not aligned, the secure message will not be revealed. (b) In contrast, our system tolerates such minor misalignment by diffusing the second share using the normalized probabilities. Both images are captured with Magic Leap One's Capture Service. Visual tracking is enabled for aligning the two shares in the head-mounted display but we still observe a slight jitter that throws off the conventional visual cryptography.

2 Algorithms

In [4], we have introduced the core algorithm of T^2VC. We present the code and discuss the parameters used in our algorithm here.

2.1 Preprocessing

Following [1] and [12], given a confidential visual image $\boldsymbol{I}$, we first generate a binary image $\hat{\boldsymbol{I}}$ by thesholding every 2×2 block of pixels in $\boldsymbol{I}$. Here, we denote $\mathscr{F}(\hat{\boldsymbol{I}})$ and $\mathscr{B}(\hat{\boldsymbol{I}})$ as the set of foreground (white) and background (black) pixels of $\hat{\boldsymbol{I}}$, respectively.

Next, we model the range of misalignment as an $s \times s$ square. We generate an $s \times s$ 2D Gaussian kernel $\mathscr{G}(x, y, \sigma)$ at scale σ:

$$\mathscr{G}(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{1}$$

where σ indicates the standard deviation of the misalignment. In our experiments, we choose $s = 3, \sigma = 1.0$ and $s = 5, \sigma = 2.0$. To model the probabilities of misalignment, we accumulate the probability to turn white for each foreground (white) pixel as follows:

```
#pragma omp parallel for
for (int i = 0; i < src.rows / block_size; ++i)
for (int j = 0; j < src.cols / block_size; ++j)
if (blocks[i][j].is_foreground) {
  auto b = &blocks[i][j];
  for (int y = i - dy; y <= i + dy; ++y)
  if (y >= 0 && y < src.rows / block_size)
    for (int x = j - dx; x <= j + dx; ++x)
    if (x >= 0 && x < src.cols / block_size) {
      auto c = &candidates[y][x][b->candidate_cnt];
      int dy = abs(i - y), dx = abs(j - x);
      c->label = share1_label[i][j];
      c->is_foreground = b->is_foreground;
      c->contribution = gaussian_foreground
        [dy + KERNEL_HALF][dx + KERNEL_HALF];
      b->prob_sum += c->contribution;
      ++b->candidate_cnt;
    }
}
```

2.2 Generation of Two Shares

T^2VC generates the first share as the classical VC approach, as shown in Fig. 4. For each 2×2 block of pixels in the first share, we randomly choose one of the six VC patterns. Next, we carry out two solutions to deal with the possible misalignment:

1. T^2VC^*: for the second share, we only diffuse the foreground pixels: each foreground pixel has a probability to be misaligned with one of its surrounding pixels; in this way, when the two shares match perfectly, the background is unchanged, but the foreground becomes darker. Please enable and disable the `GENERATE_GAUSSIAN_KERNEL` macro to compare with the classic algorithm.

2. T^2VC: for the second share, we diffuse both the background and foreground pixels to enhance the contrast: every pixel has a probability to be misaligned with one of its surrounding pixels. Please enable the `SPREAD_ALSO_FROM_BACKGROUND` macro to see the results in the supplementary code.

The pseudo code of the core algorithm is shown in Algorithm 1 and the source code is provided in the supplementary material.

3 Experimental Results

To valid the effectiveness of our algorithm, we conduct preliminary experiments via both simulation and physical deployment on a Magic Leap One.

3.1 Comparison with Classical Visual Cryptography

Considering that the resolution of Magic Leap One is 1280×960 pixels, we generate visual cryptography images at the resolution of 1024×1024 pixels using a custom C++ program using the proposed T^2VC algorithm, as well as the classical visual cryptography algorithm. We first evaluate our system by simulating the misalignment under four conditions: exact match, one-row misalignment (R1), one-column misalignment (C1), and one-row, one-column misalignment (R1+C1).

As shown in Fig. 4, we arrive at the following insights:

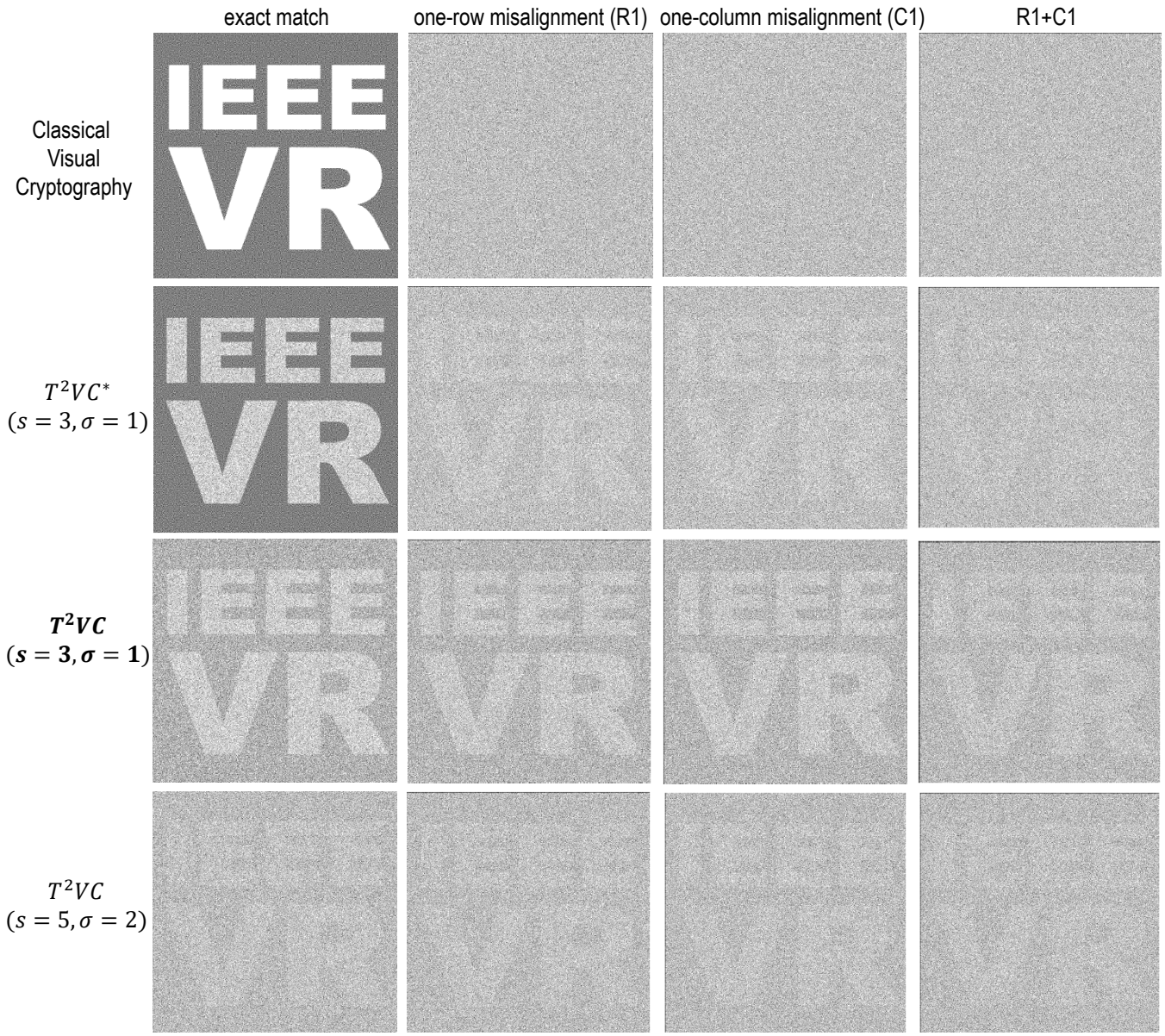


Figure 4: Results among the classical visual cryptography approach and T^2VC approaches with different parameters (s indicates the size of the Gaussian kernel, σ indicates the standard deviation of the Gaussian kernel). From the results, we observe that both T^2VC and T^2VC^* outperform the visual cryptography algorithm in R1 or C1 cases. T^2VC provides better contrast than T^2VC^* when both R1 and C1 misalignment occur.

1. The classical visual cryptography algorithm does not work with even a single row or column of misalignment, making it extremely challenging to interpret the image with even the slightest error in visual tracking.

2. T^2VC^* can deal with one row or one column misalignment (2 pixels) while preserving as good a contrast as the original visual cryptography algorithm with no misalignment. However, the contrast lowers with misalignment.

3. T^2VC provides better contrast than T^2VC^* when misalignment occurs and even works for the R1+C1 case (two pixels misaligned both horizontally and vertically). After increasing the size and scale of the Gaussian kernel, we can still see the secret message even with two rows (four pixels) of misalignment.

3.2 Deployment

We have implemented our system in Unity and deploy it on Magic Leap One and Microsoft HoloLens. Magic Leap One is equipped with built-in visual tracking modules while Microsoft HoloLens only supports stabilizing an image in the 3D space. We present two examples in Fig. 5 using the T^2VC algorithm ($s = 3, \sigma = 1$), with one share in the head-mounted display and the other share displayed in a desktop monitor or printed in a piece of paper. With T^2VC, we can still observe the fused image even when the visual tracking module of Magic Leap One misaligns the two shares.

(a) revealing a teacup icon with one share displayed on a desktop monitor

(b) revealing two characters *VR* with one share printed on a piece of paper

Figure 5: (a) This figure shows the results by seeing through Magic Leap One to watch the other share (a) in a desktop monitor, and (b) on a piece of paper.

Human vision system is sensitive to both static and temporal contrasts. Therefore, we suggest smoothly changing the brightness level of the overlaid image. Fig. 6 presents a series of frames of fusing two shares of images in Magic Leap One at different brightness levels. Since the gradient values of the foreground and background differs over the time, the secure message becomes more salient in the temporal domain. Please refer to the video for more detail.

Figure 6: Changing the brightness of the overlaid image over the time may assist the user to recognize the secure message easily.

4 Conclusion

In this paper, we have adapted visual cryptography for current-generation augmented reality headsets. Our system T^2VC uses a novel visual cryptography algorithm which is tolerant to users' head jitter and slight misalignment of the two shares of encrypted visual information when visual tracking is enabled. We achieve this by modeling the misalignment through a 2D Gaussian distribution of the visual cryptography's random patterns. This allows us to trade off precise alignment with perceived contrast. As one of the first steps towards practical visual cryptography for virtual and augmented reality, we believe that our algorithm provides a versatile, commodity, off-the-shelf solution for embedding encrypted augmented reality information in both the real-world displays and virtual environments [3,5], thereby protecting confidential data while facilitating an easy-to-use visual decryption.

Acknowledgement

We would also like to thank *Cheng Tan* for the initial discussion of visual cryptography and the anonymous reviewers for the insightful feedback.

This work has been supported in part by the NSF Grants 1823321, 1564212, 1429404, and the State of Maryland's MPower initiative. Any opinions, findings, conclusions, or recommendations expressed in this article are those of the authors and do not necessarily reflect the views of the research sponsors.

References

[1] S. J. Andrabi, M. K. Reiter, and C. Sturton. Usability of Augmented Reality for Revealing Secret Messages to Users But Not Their Devices. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pp. 89–102, 2015.

[2] C. Blundo, A. De Santis, and M. Naor. Visual Cryptography for Grey Level Images. *Information Processing Letters*, 75(6):255–259, 2000. doi: 10.1016/S0020

[3] R. Du. *Fusing Multimedia Data Into Dynamic Virtual Environments*. PhD thesis, University of Maryland, College Park, Nov. 2018.

[4] R. Du, E. Lee, and A. Varshney. Tracking-Tolerent Visual Cryptography. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces*, VR, p. 2, Mar. 2019.

[5] R. Du, D. Li, and A. Varshney. Geollery: a Mixed Reality Social Media Platform. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI)*, CHI, p. 13. ACM, May. 2019. doi: 10.1145/3290605.3300915

[6] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, et al. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pp. 475–488. ACM, 2014. doi: 10.1145/2663716.2663755

[7] Y.-C. Hou. Visual Cryptography for Color Images. *Pattern Recognition*, 36(7):1619–1629, 2003. doi: 10.1109/COMPTELIX.2017.8003979

[8] B. Liu, R. R. Martin, J.-W. Huang, and S.-M. Hu. Structure Aware Visual Cryptography. *Computer Graphics Forum*, 33(7):141–150, 2014. doi: 10.1111/cgf.12482

[9] D. Liu, E. Cuervo, V. Pistol, R. Scudellari, and L. P. Cox. Screenpass: Secure Password Entry on Touchscreen Devices. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 291–304. ACM, 2013. doi: 10.1145/2470654.2481331

[10] M. A. Livingston, J. L. Gabbard, J. E. Swan II, C. M. Sibley, and J. H. Barrow. Basic Perception in Head-Worn Augmented Reality Displays. In *Human Factors in Augmented Reality Environments*, pp. 35–65. Springer, 2013. doi: 10.1007/978-1-4614-4205-_3

[11] C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun. Smartphones As Practical and Secure Location Verification Tokens for Payments. In *The Network and Distributed System Security Symposium (NDSS)*, 2014.

[12] M. Naor and A. Shamir. Visual Cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 1–12. Springer, 1994. doi: 10.1109/ICRITO.2016.7784984

[13] Z. Zhou, G. R. Arce, and G. Di Crescenzo. Halftone Visual Cryptography. *IEEE Transactions on Image Processing*, 15(8):2441–2453, 2006. doi: 10.1109/TIP.2006.875249