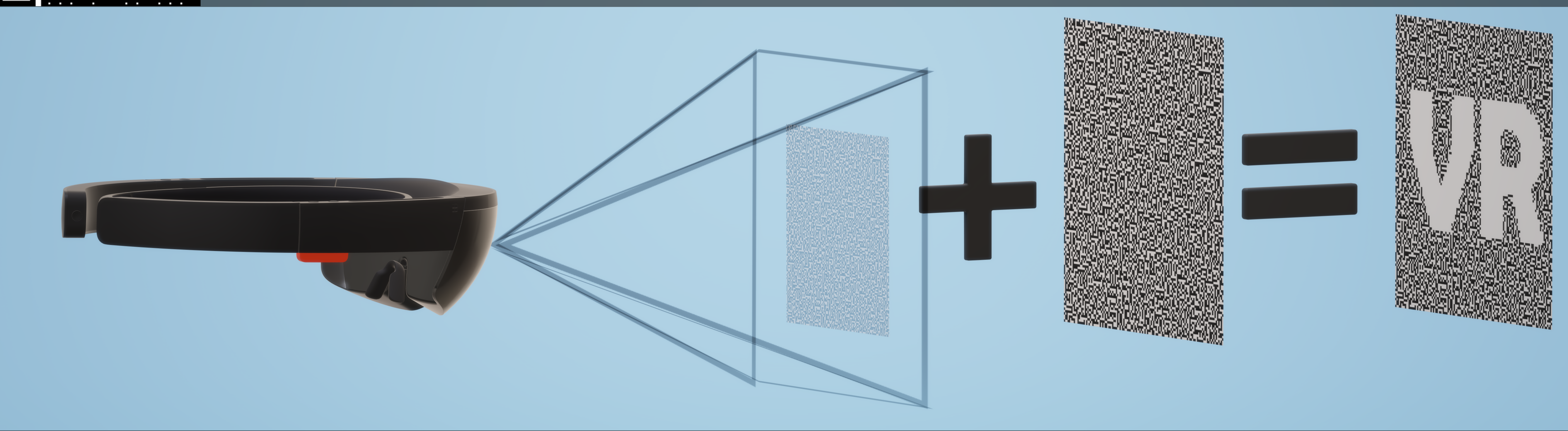
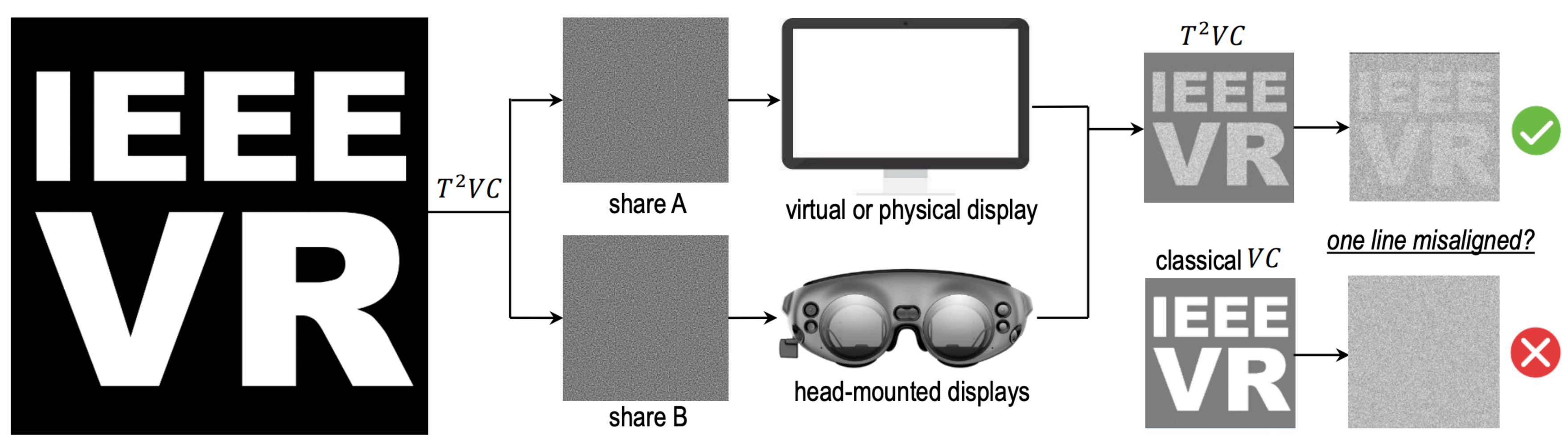
T^2VC Tracking-Tolerant Visual Cryptography



Ruofei Du, Eric Lee, and Amitabh Varshney

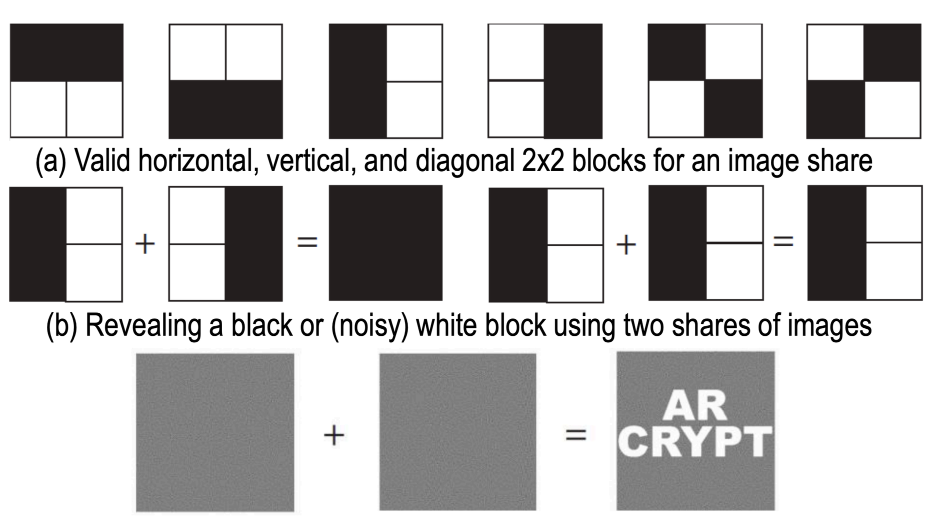
Introduction

We introduce T²VC, a novel secure display system which uses visual cryptography (VC) with tolerance for tracking. Our system brings cryptographic privacy from text to virtual worlds. 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 with both images is able to visually decrypt the data by fusing them. 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.



Algorithm

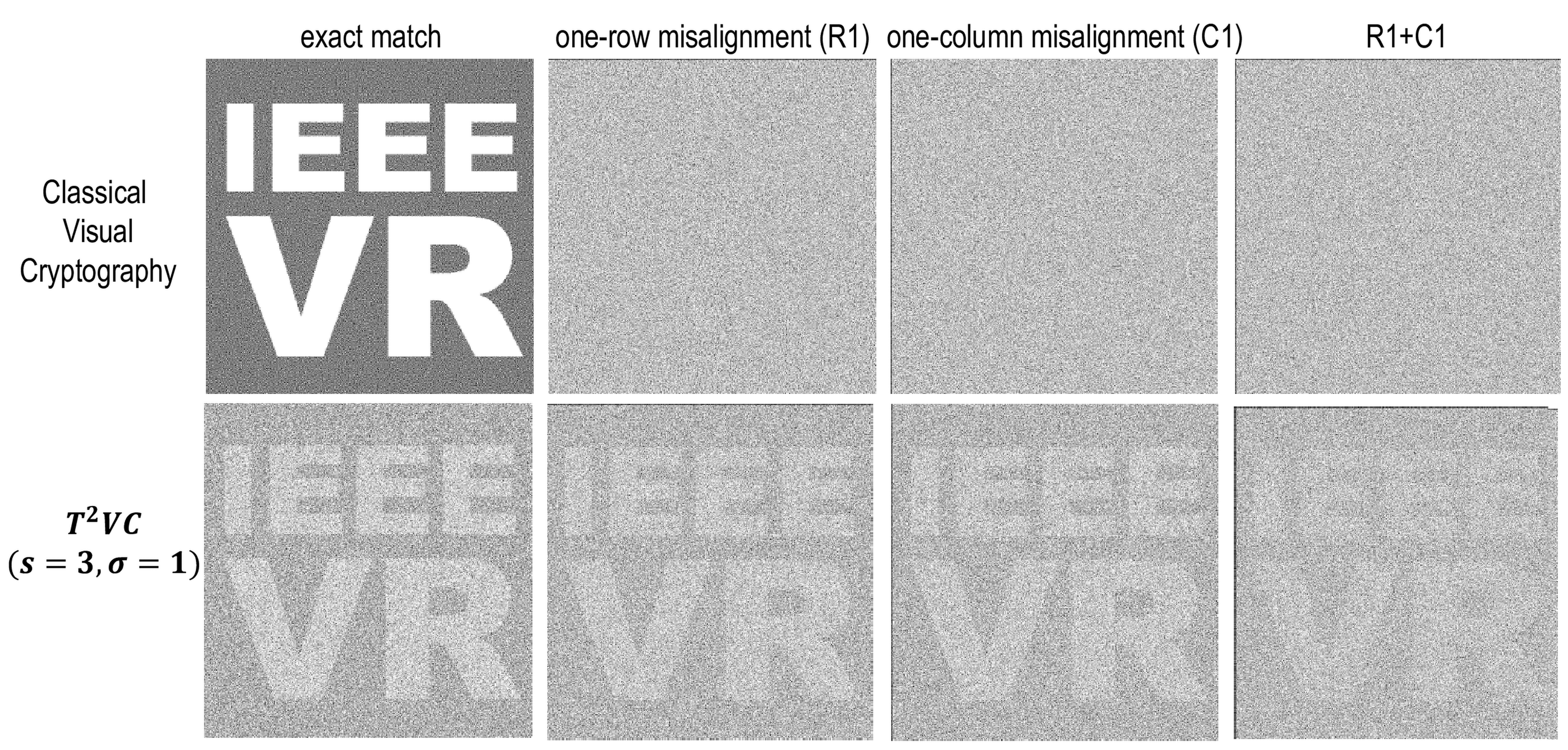
In 1994, Moni Naor and Adi Shamir developed the first VC framework. However, it is challenging to perfectly align the two shares in AR head-mounted displays. In T²VC, we model the probability of misalignment as a Gaussian distribution and diffuse the pixel colors of the second share using a Gaussian kernel.



(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

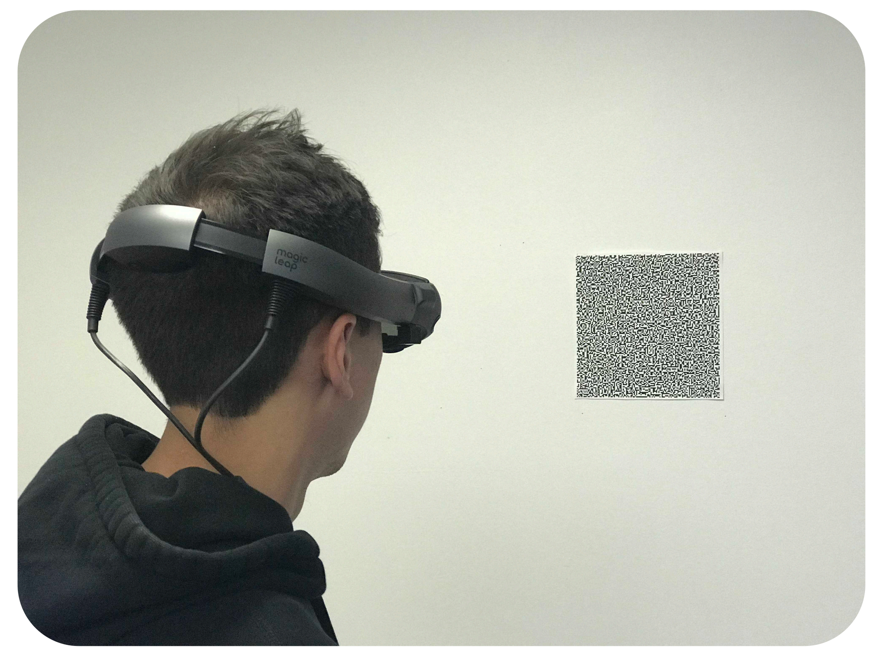
(c) A concrete example of classic visual cryptography

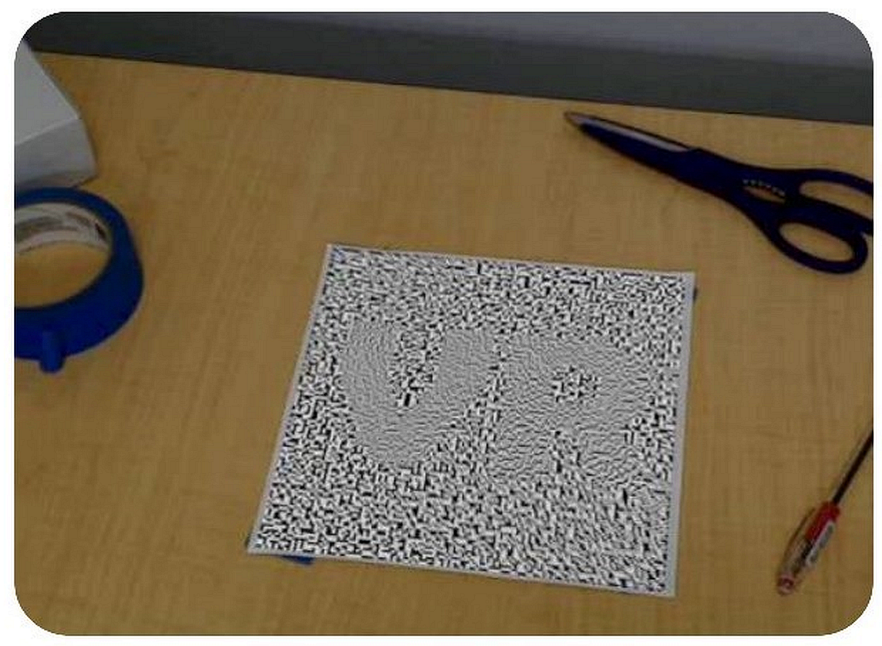


Experimental Results

We have implemented our system in Unity and deploy it on Magic Leap One AR headset. One of the generated shares is placed in the physical world, *i.e.*, printed on a piece of paper or displayed on an ordinary monitor. The other share is rendered and displayed by the headset. We use visual tracking to estimate the position and rotation of the physical share and transform the headset's share to align. This decouples alignment from the user's relative location.

Note that the classical VC algorithm does not work with even a single column or row of misalignment, making it extremely challenging to interpret the image with even the slightest error in visual tracking. In contrast, T²VC allows us to trade off precise alignment with the perceived contrast. As a result, users can still interpret the fused image even when the visual tracking misaligns the two shares.

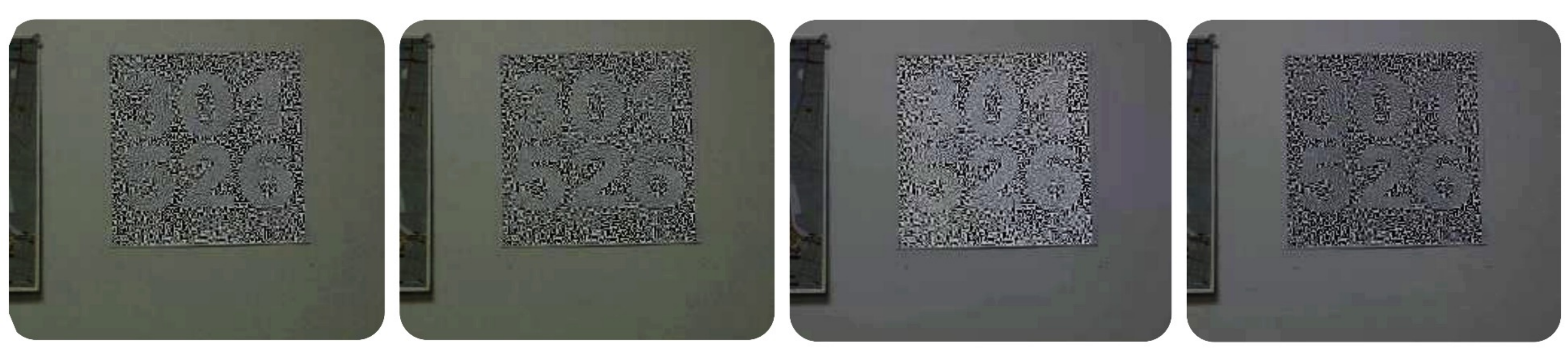




Conclusion and Future Work

In this paper, we have adapted visual cryptography for the current generation augmented reality headsets. Our system, T²VC, uses a novel visual cryptography algorithm which is tolerant to users' head jitter and slight misalignment of the two shares of encrypted. data As a first step 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 real-world displays and virtual environments, thereby protecting confidential data while facilitating an easy-to-use visual decryption.

Although our algorithm is robust to conditions cause by the use of AR headsets, our system trades perceived contrast for reduced alignment precision while further work may evaluate methods to increase contrast, *e.g.*, changing the brightness over time.



University of Maryland

UMIACS

THE AUGMENTARIUM
VIRTUAL AND AUGMENTED REALITY LAB
AT THE UNIVERSITY OF MARYLAND

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND