Moiré cryptography.

Conference Paper · November 2000

DOI: 10.1145/352600.352618 · Source: DBLP

2 authors, including:

Tri Le
BMC
29 PUBLICATIONS **738** CITATIONS

Moiré Cryptography

Yvo Desmedt
Department of Computer Science
PO Box 4530, Florida State University
Tallahassee, FL 32306, USA, and

Royal Holloway College
University of London, UK.
desmedt@cs.fsu.edu

Tri Van Le
Department of Computer Science
PO Box 4530, Florida State University
Tallahassee, FL 32306, USA.
levan@cs.fsu.edu

ABSTRACT

As already pointed out by other researchers, one of the central problems with applicability of visual cryptography is the random nature of its secret shares. It makes secret shares not suited for carrying or for transmission over an open channel. In this paper, we apply concepts of steganography to create secret sharing schemes whose shares are realistically looking images. Our new technique is based on an idea of employing Moiré patterns for producing images. The advantage of this scheme over others is that it does not require a complicated algorithm, thus a computer, to decrypt the ciphertext. The cleartext can be read simply by putting the ciphertexts one onto the other. We therefore give a solution to the above mentioned problem with a novel type of visual secret sharing schemes, whose secrecy and anonymity are both satisfied.

Keywords: steganography, privacy and anonymity, information hiding.

1. INTRODUCTION

In the increasingly connected modern world, one may wish to be able to protect not only secrecy of the communication but also privacy of the communicators. Anonymous communication allows one to communicate without revealing who is communicating [4]. The so called *dining cryptographers problem* [5] is a known one of such schemes. It is a broadcasting solution that protect sender and receiver's anonymity. In this approach, a sender broadcasts his messages to all his neighbors. The network bandwidth needed therefore is very high. However, one may communicate with both anonymity and better bandwidth efficiency, such as in the *onion routing scheme* [8]. In this proposed solution, the path of each data packet is computed before sending. By applying several layers of encryptions to each individual packet, each router on the packet's path is able to access to the information needed for it to forward the packet only, i.e. the immediate destination of the packet. This approach has an advantage that the bandwidth needed is limited. However network routers need to do more work, i.e. decrypting then striping off headers of each packet. Importantly, the scheme is only secure if the routers are not able to collude. If the routers are able to collude then the original sender and receiver may be revealed.

Steganography and information hiding, which is as old as cryptography [10], allows one to communicate privately *in plain*. In more details, the sender embeds a secret communication channel in another open channel, possibly a monitored one. With this setting, the embedder is able to send a secret message to a receiver without any trace. In this paper we show how we applied this idea to create Moiré cryptography, a novel type of of visual secret sharing (described bellow) which has both content secrecy and communicator anonymity.

Visual cryptography introduced in the open literature in [11] is a novel approach to realize cryptography. It has a very attractive feature that its ciphertexts are transparencies, which are readily to be decrypted with an overhead projector. To decrypt the ciphertexts, one places one transparency onto the other and the cleartext is revealed. No computer is needed in the decryption.

Details of the visual encryption follows (see [3, 12] for terminology). Let the secret be a black and white picture. If a point in the secret is black, that point is encoded:

- with probability 1/2, as an L block in the first share, and as an R block in the second share.
- with probability 1/2, as an R block in the first share, and as an L block in the second share.

Here L is the square in Figure 1, and R is the square in Figure 2. Otherwise, if a point in the secret picture is white then that point is encoded:

- with probability 1/2, as an L block in the first share, and as an L block in the second share.
- with probability 1/2, as an R block in the first share, and as an R block in the second share.

To decrypt, one stacks one transparency onto the other. The secret picture then shows up in the following manner. Each black point is shown as a completely black block, while

CCS'00, Athens, Greece.

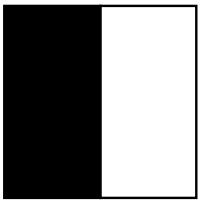

Figure 1: L block.

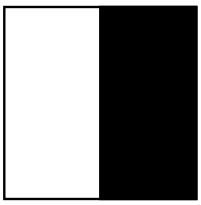

Figure 2: R block.

each white point is shown randomly as one of the two blocks L and R in Figure 1 and Figure 2, respectively. Receiver needs to stack carefully two transparencies together so that blocks in the shares are correctly paired.

The lack of a computer in the decryption process is an inherent security advantage. Computers are commonly known not trusted for keeping highly valued data such as secrets and sensitive information in plain form. A high density processor with millions of transistors may contains bugs. Even worse, they may contain purposely implanted bugs. These bugs are known of being able to secretly *leak* sensitive data or secret keys to the network, or to some unknown outsider. This situation is possible if the computer used by a receiver to decrypt or to view the secret is under control of some adversary. It is even more difficult to know whether this is really the case when some part(s) of the computer (e.g. the processors, cryptographic devices) are sold to end users as black-boxes. Therefore having no computer in decrypting and in viewing the message closes this gap in the system's security.

However, the research on visual cryptography has been focussed mainly on guaranteeing secrecy but not anonymity. Therefore, an inherent disadvantage of visual cryptography, as already pointed out in [7], is that random transparencies are suspicious and susceptible to censorship. Anyone would find it embarrassing to be discovered carrying random transparencies.

Recent progress has addressed this issue in visual cryptography [2]. One solution is to modify the shares in such a way that they should differ critically from images of random dots. For example, in [1], the authors argued that since their shares have some meaning to a general viewer, it may help users in carrying the secret shares. However, their shares are still far from real images. They look random enough to allow a censor to block the delivery.

In optical cryptography [6], secret shares are real images. However, the receiver needs special devices called Mach-Zehnder interforemeters to decrypt the ciphertexts. Similarly, in cerebral cryptography [7], the receiver uses a 3D stereo viewer instead of an interforemeter to view cleartext. Since these devices are not widely available, one may need to carry these devices together with the shares.

In this paper, we apply concepts of steganography [10] to solve the above problems in a satisfactory manner. We produce secret shares which are normal pictures in such a way that by stacking one picture onto the other, the secret image is revealed. From human visual sensor's perspective, our scheme's shares look like real pictures, so it solves anonymity problem mentioned in the preceeding paragraph. Furthermore, our scheme is perfectly secure, meaning that given any single share, no information about the secret is leaked.

The paper is organized as follows. In Section 2, we review concepts and techniques used later in the paper. In particular, we describe principles of modern printers, and aliasing effects. While these effects are avoided in computer graphics, they turn out to be perfectly useful for our embedding purposes. In Section 3, we first discuss several ideas that lead to our Moiré scheme, which is described in the later part of the section. In the last Section 4, we give a sample output of our scheme and complete our paper with some open questions.

2. CONCEPTS AND TECHNIQUES

This section is devoted to concepts and techniques that will be used later in our paper.

2.1 Digital Printers

Many modern printers represent rasterized images as a bitmap. Each pixel in the real image corresponds to a convex area called a dot in the output, such as a disc or a square of some given color. Non-basic colors are composed by combining several dots in basic colors printed nearby each other. Gray images are first *half-toned* and then printed on black-white printers. The dots are placed in a regular two dimensional lattice. Regular lattices introduce minimal noticeable artifacts to the hard copy. The density of the lattice may be as low as 75dpi in dot matrix printers or as high as 1800dpi in laser jet printers. The higher the density is, the better the images are. Normal desktop printers have density of 600-1200dpi. The use of a regular lattice also leads to a special aliasing effect called Moiré effect. This effect occurs when high frequency lattices are combined together to produce very low frequency lattice pattern, such as shown in Figure 3. The corresponding aliasing effect in one dimension case is shown in Figure 4 (see [9].) In Figure 4, a wave of frequency 10Hz is sampled at 11Hz. The result is a wave of 1Hz. Note that superposition of two transparencies is a multiplicative operation where 1 is white and 0 is black. In other words, it is the re-sampling of one transparency at the transparent locations of another transparency. Therefore we see the same effect happening in the two dimensional case.

2.2 Moiré Cryptography Model

We illustrate the model of Moiré cryptography in Figure 5. In this figure, the character **R** stands for the operation of randomizing embedded picture into two random preshares, each is independent of the embedded picture, and whose combination (with an exclusive-or operation) is the embedded picture. This is the standard one-time-pad technique. It is done by choosing the first preshare uniformly random. The second preshare will then be embedded picture *xor* the first preshare.

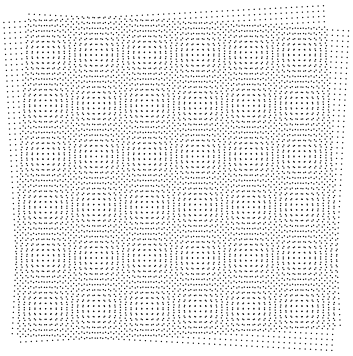

Figure 3: ***Moiré pattern in two dimensions.***

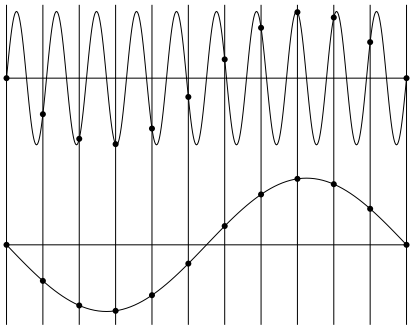

Figure 4: ***Aliasing pattern in one dimension.***

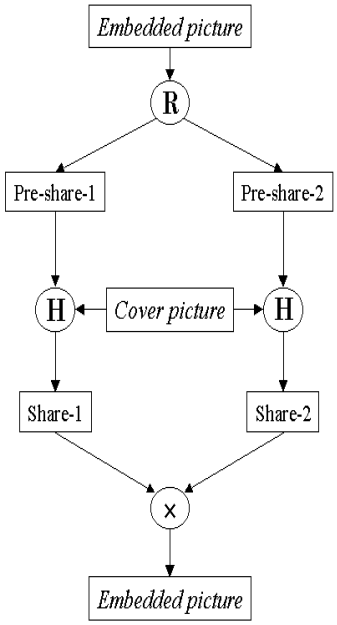

Figure 5: ***Model of Moiré cryptography.***

The character **H** in the picture stands for the hiding algorithm. It takes two arguments, a cover picture and a random (monochrome) pre-share, and output the corresponding share. The algorithm formats the cover picture accordingly to the pre-share. It does this by copying (while modifying) each dot in the the cover picture into the share, drawing the new dots in diamond shapes. The darker the point on the cover is, the bigger is the diamond on the share. On the other hand, if the point in the pattern is black, then the diamond is pointing northwest to southeast, otherwise it is pointing southwest to northeast. These diamonds are shown on Figure 6. The upper ones correspond to black dots while the lower ones correspond to a white dots of the pre-share.

The resulting share now looks the same as the input cover picture because each point in the cover picture is copied to the same location and with the same size (same area) in the resulting picture. The only difference is that the points are no longer circles but diamonds. Hence all the frequencies lower than the sampling frequency (i.e. the frequency of dots in the picture) is unchanged. When the dots are small enough, i.e. the sampling frequency is high, this difference is un-noticeable to the eyes.

To recover the embedded picture, the shares are combined together by superimposing one onto another. This is noted as the $\times$ operation in the picture. If we denote 0 for the black dots and 1 for the white dots, then the superimposing operation on the transparencies is really a multiplicative dot operation.

In the next Section, we will study how these dots form the embedded picture with the Moiré effect.

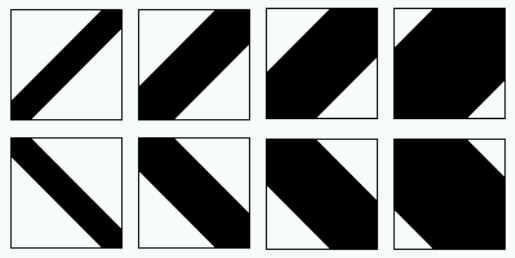

Figure 6: ***Hiding dots.***

3. MOIRÉ VISUAL SCHEMES

In this Section, we introduce several Moiré visual cryptographic schemes, raising from simple to more complicated ones. Constructing a working scheme is nevertheless not simple, as our discussion will reveal later.

3.1 Moiré schemes

3.1.1 Main Ideas

When we stack two transparencies together, the result is an *and* operation of the two transparencies. Unfortunately, this does not provide a group operation on the set $\{0, 1\}$, thus it can not provide perfect secrecy. Visual cryptography overcame this by encoding 0 and 1 with random black-white matrices of different averaged gray levels.

Here we propose another method using the Moiré effect. To encode a bit, one uses different Moiré patterns. As we noted earlier in Section 2, Moiré patterns depend on the relative difference in high frequencies of the two transparencies. This difference can be controlled by the relative angle between the two transparencies. This observation motivates the following Moiré schemes.

Lattice rotation

In this scheme, we rotate areas of the output lattices differently so that black areas in secret image correspond to one Moiré pattern, while white areas in secret image correspond to another Moiré pattern on the superposition of the two transparencies. This scheme produces very clear and sharp decrypted ciphertext. However the boundary between differently-rotated areas in the shares is visible.

Lattice smooth rotation

Having seen the problem with previous scheme, we try to rotate the areas in the lattice smoothly so that there are no real boundary among differently-rotated areas. This did overcome the visibility disadvantage of the previous scheme. However it introduced new problem. It turns out that albeit the real boundary is invisible, the artifacts introduced into the shares (by the rotated lattice) stand out too much and are now visible.

Dot orientation

In the previous two schemes, we have seen that rotating parts of the lattice is not a very good idea. This suggests us that we need something else. We came to some other solution, namely instead of rotating the lattice, we orient the printed dots. In order to do that, first we have to make the dots in some orientable shapes such as diamonds or ellipses. One may think that the ellipse shape is better because it looks more natural to the original circle. We tried both types of shapes and our result shows that although both shapes are good, in fact the diamond dots introduced less visible boundary than the ellipse dots. The diamond dots are shown in Figure 6. Note that dots of higher gray levels correspond to bigger diamonds in the figure.

Now to encode a 1 bit, we superimpose two squares on the two shares, whose dots are oriented with different angles. To encode a 0 bit, we superimpose two small squares on the two shares, whose dots are oriented by the the same angle. Hence the resulting picture appears with one Moiré pattern for the black dots and another Moiré pattern for the white dots. Hence in this scheme it is the Moiré pattern that form the embedded picture; not the gray level of the squares as done in visual cryptography.

3.1.2 Encryption

THEOREM 1. *Let C and E be the cover and embedded pictures, respectively. Then the shares S_1 and S_2 determined by the following algorithm:*

1. *Let $q \in_R \{0,1\}^{n \times n}$, and $q' := q$ xor E.*
2. *Let $S_1 := H(C, q)$.*
3. *Let $S_2 := H(C, q')$.*

satisfy these conditions:

- *i. Perfect secrecy: S_1 and S_2 are independent of E.*
- *ii. High quality: $S_1 \approx S_2 \approx C$.*
- *iii. Decryptable: Moiré(S_1, S_2) looks like E.*

where H is the hiding algorithm described in Section 2.2.

Proof

The proofs of *(i)* and *(ii)* follow from our discussions ealier, while proof of *(iii)* is shown in the following decryption section.

3.1.3 Decryption

The decryption process is relatively simple. We stack the two transparency onto each other to create Moiré patterns.

When $E_{ij} = 0$, the dots of S_1 and S_2 inside the square (i, j) will point to the same direction, i.e. either LL or RR. This gives a Moiré pattern of the first type.

When $E_{ij} = 1$, the dots of S_1 and S_2 inside the square (i, j) will point to different directions, i.e. either LR or RL. This gives a Moiré pattern of the second type, with texture different from that of the Moiré pattern of the first type (because the angle between two squares is now different).

The embedded picture E is now be visible in the Moiré pattern, the black area of the picture E corresponds to texture of the first type, while the white area of the picture E corresponds to texture of the second type. The two types of textures are visually different so we *see* the picture E.

3.2 Discussions

We give some sample output of our scheme here. The original cover image is the picture of a bottle of flowers in Figure 7. The corresponding secret shares are given in Figure 8 and Figure 9, respectively. These shares when combined will show the bold text **FSU** at the center of the transparency in dark color. The text is surrounded by a rectangle with lighter background. A simulated output of this combination is given in Figure 10. We used squares of 8 by 8 dots to make oriented dots on printouts, which were printed at 1200 dpi.

Moiré patterns are stable with respect to certain amount of rotation and translation. Even if the transparencies are misplaced or rotated, the Moiré pattern still occurs, i.e.

Figure 7: *Original picture.*

Figure 8: *First share.*

Figure 9: *Second share.*

Figure 10: *Simulated decryption.*

the embedded picture can still be seen. In fact, experiments have demonstrated that when one transparency is moving relatively to the other, the embedded picture becomes clearer. Thus besides using only real pictures as secret shares, Moiré schemes are also robust against missed placement and/or orientation.

4. SUMMARY

The introduction of computers made complicated steganographic algorithms more practical. These algorithms offer many more good properties than the original techniques can do, for example ease of use and proven secrecy. In this work, we have shown that one can achieve both perfect secrecy and anonymity in visual secret sharing schemes. Several aspects have been addressed together in this paper, i.e. absence of computers in decryption of ciphertexts, secrecy, and anonymity. Making higher contrast to the scheme is left for future work. Our work opens a question of whether we can use this same method for purposes other than encryption, for instance authentication. The existence of similar schemes providing proven (i.e. unconditional or computational) undetectability is open.

Acknowledgements

This work was partially supported by the National Science Foundation with grants NSF CCR-9508528 and NSF CCR-9903216. Part of this work was done while the authors were at the University of Wisconsin-Milwaukee.

A. REFERENCES

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, to appear.

[2] E. Biham, September 21–26, 1997. Lecture given at Daghstuhl, Germany.

[3] G. R. Blakley. Safeguarding cryptographic keys. In Richard E. Merwin, Jacqueline T. Zanca, and Merlin. Smith, editors, *1979 National Computer Conference: June 4–7, 1979, New York, New York*, volume 48 of *AFIPS Conference proceedings*, pages 313–317, Montvale, NJ, USA, 1979. AFIPS Press.

[4] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[5] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):65–75, 1988.

[6] Y. Desmedt, S. Hou, and J.-J. Quisquater. Audio and optical cryptography. In K. Ohta and D. Pei, editors, *Advances in Cryptology — Asiacrypt '98, Proceedings (Lecture Notes in Computer Science 1514)*, pages 392–404. Springer-Verlag, October, 18–22 1998. Beijing, China.

[7] Y. G. Desmedt, S. Hou, and J.-J. Quisquater. Cerebral cryptography. In D. Aucsmith, editor, *Information Hiding, Second International Workshop, Proceedings (Lecture Notes in Computer Science 1525)*, pages 62–72. Springer-Verlag, 1998. Portland, Oregon, April 15–17.

[8] David Goldschlag, Michael Reed, and Paul Syverson. Internet privacy - onion routing for anonymous and private internet connections. *Communications of the ACM*, 42(2), 1999.

[9] Bernd Jahne. *Digital Image Processing: Concepts, Algorithms, and Scientific Applications.* Springer-Verlag, Berlin, Heidenberg, third edition, 1998.

[10] David Kahn. *The codebreakers: the story of secret writing.* MacMillan Publishing Company, New York, NY, USA, 1967.

[11] M. Naor and A. Shamir. Visual cryptography. In Alfredo De Santis, editor, *Advances in cryptology — EUROCRYPT '94: Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9–12, 1994: proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 1–12, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. Springer-Verlag.

[12] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979.