MANTECH Publications

Journal of Digital Image Processing and Computer Vision
Volume 3 Issue 1

Visual Cryptography and its Challenges

Suchethana H C
Department of Information science and Engineering
JNNCE, Shivamogga, India
***Corresponding Authors' email id**: suchethanahc@jnnce.ac.in*

Abstract

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields. Visual Cryptography comes in the field of data hiding used in cybercrime, file formats etc. This paper focuses on the application areas of visual cryptography about the most important application areas of visual cryptography. Visual cryptography can be used to protect biometric templates in which decryption does not require any complex computations. a secret image which is encoded into N shares printed on transparencies. The shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye. Some challenges of visual cryptography example the contrast of the reconstructed image,perfect alinment of the transferencies are projected.

***Keywords:** Halftoning, Cyber Theft, Chiper text, Encryption, Decryption, Cipher images, Sub pixel, Stegnography, Watermarking*

I. INTRODUCTION

Visual Cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In today's computer generation, data

security, hiding and all such activities have become probably the most important aspect for most organizations. These organizations spend millions of their currency to just secure their data. This urgency has risen due to increase in cyber theft/ crime. The technology has grown so much that criminals have found multiple ways to perform cyber crime to which the concerned authorities have either less or not sufficient answer to counter. Hence, the method of Cryptography provides the above answers. One of the most major parts of cryptography is Visual cryptography. It has many usage & application areas, mostly using its internal technique called encryption. Some of those application areas are talked about in this research paper. Visual cryptography is used specifically in the areas of Biometric security, Watermarking, Remote electronic voting, Bank customer identification etc. quality is poor.

In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm [2] to encode a secret binary image into n halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares are observably better than that attained by any available visual cryptography method known to date. Cryptography refers to the study of mathematical techniques and related aspects of information security like data confidentiality, data integrity and of data authentication. In the process of Visual Cryptography a secret image is encrypted into shares which refuse to divulge information about the original secret image. Decryption is through a separate decryption algorithm. A basic model for Visual Cryptography for natural images was proposed by Naor and Shamir, where the resultant image is twice the size of secret image.

As the advent of electronic applications increases, providing the security for information in an open network environment is required. Encryption is a method of transforming original data, called plain text or clear text into a form that appears to be random and unreadable which is called Cipher text. Plain text is either in the form that can be understood by a person (document) or by a computer (executable code). Once it is transformed into Cipher text, neither human nor machine can properly process it until it is decrypted. This enables the transmission

of confidential information over insecure channels without unauthorized disclosure. When data is stored on a computer it is protected by logical and physical access controls. When this same sensitive information is sent over a network,the information is in much more vulnerable state.

Naor and Shamir introduced the new concept of Visual Cryptography in 1994[1], requiring no computation except human Visual System to decrypt. They proposed a basic (2,2) Visual Cryptography scheme where a secret image is divided into 2 shares, revealing the secret image through Share Stacking.

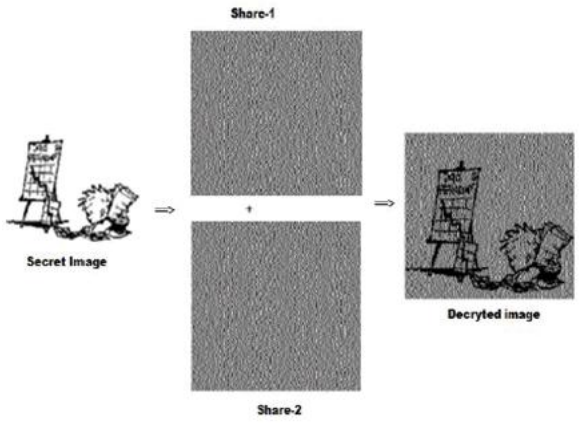


Fig: 1 Example of Visual Cryptography

In figure 1 a secret image that has to be sent is divided into shares. When these two shares are stacked together and put into a Human Visual System the resultant image is revealed.In the visual secret sharing model [1], a secret picture must be shared among n participants. The picture is divided into n shares so that if m transparencies (shares) are placed together the picture is visible. When there are fewer m transparencies it is invisible. This ensures that the secret picture is viewed as a set of black and white pixels with each pixel being handled separately.

RELATED WORK

2.1 Basic (2, 2) Scheme

The (2, 2) VC scheme divides the secret image into two shares so that reconstruction of an image from a share is impossible. Each share is printed in transparency. A share is a random noise. Encryption is performed for each pixel. Fig.2 shows the 2 different shares for black and white pixels. The figure shows how a pixel in a image in divided into two sub pixels depending on whether the pixel is black or white. By doing so the width of the share increases. This is termed as Pixel Expansion.

Figure 2 shows the problem of Pixel expansion where a Pixel in the image is divided into 2 sub pixels which increase the width of the entire image and thus there will be increase in bandwidth required and so increase in the power consumption.

2.2 Pseudo Randomized Visual Cryptography Scheme

Figure 3 shows how the shares are generated by pixel reversal and using pseudo random technique. Each pixel is being handled separately. The input is a secret image and the output is the shares. Here there is no pixel expansion. The decoded image and the original secret image are of the same sizes. But the secret image which is decoded had a darker resolution than the original image. Pre-processing technique was used to overcome this problem.

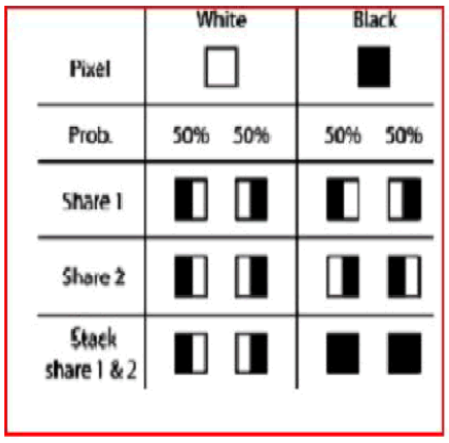


Fig. 2 A (2, 2) Visual Cryptography Scheme

PROPOSED WORK

In this paper, the problem of pixel expansion is eliminated and also a method is proposed for color image usage and thus the degradation of the resultant image is reduced. A secret image is taken and is split into RGB components. Each component is handled separately. Each pixel is decomposed using Bit Plane Decomposition technique. ATMF and De – noising is done to eliminate the presence of noise. This result is then encrypted using Chaotic Random Number Generator and the bit planes are re – ordered and Re – combined. Pixel Index Reversal is done to reverse the index of the pixel to improve the Security. At this stage Zigzag Scan Pattern is applied to increase the scrambling, thus increasing the Security. The output after the Scan is then applied to Pseudo Random Scheme as shown in Figure 3.

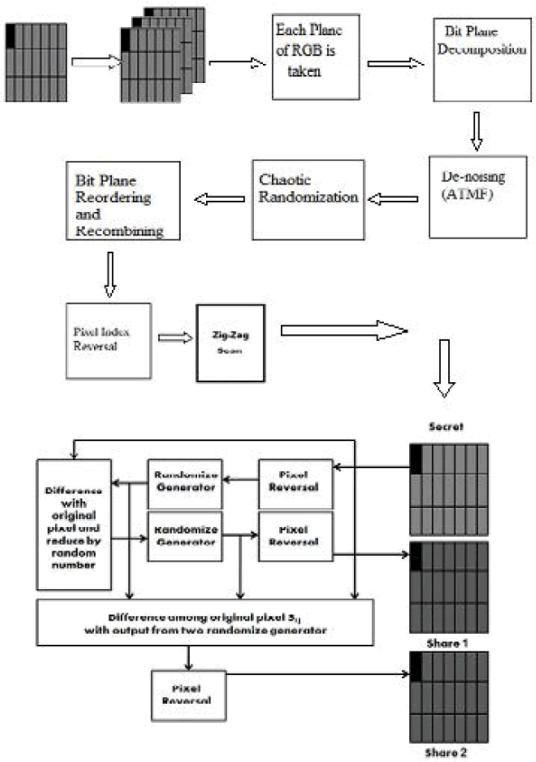


Figure: 3

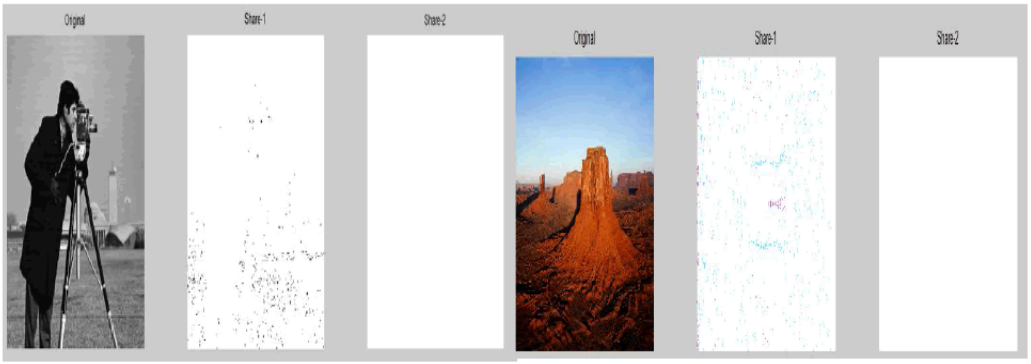


Fig. 5 Results for gray image as input Fig. 6 Results for Colour Image as input

Figure 5 shows the result for the basic concept of Visual Cryptography for a Gray Image. Figure 6 shows the results for the basic concept of Visual Cryptography for a Colour Image.

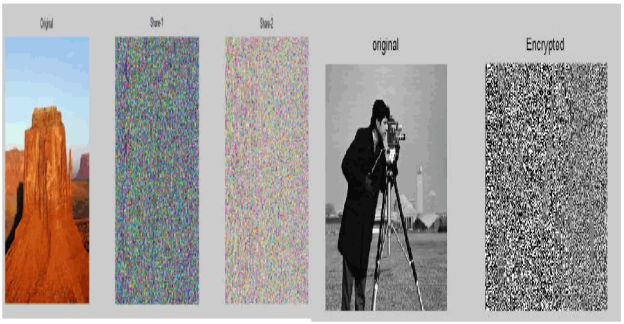


Fig. 7 Results for Colour Image after applying the Security Methods Fig.8 Completely Encrypted Image

Figure 7 shows the results of the encryption and generation of shares after applying the security measures like Pixel Index reversal, Scan pattern method, Chaotic randomization. Figure 8 shows the integration of Visual Cryptographic concept with (n, k, p) gray code concept.

3.2 Comparison of the Algorithms

Table.1 Comparison of Algorithms

Algorithm	Pixel	Security	Quality
Naor, Shamir	Double	Increase	Poor
(k,n) scheme	Double	Increase	Poor
Existing Method	No Expansion	Increase	Increase
Proposed Work	No Expansion	Increase	Color Image

The above table shows the comparison of the existing and proposed techniques of Visual Cryptography.

Example

A demonstration of visual cryptography. When two same-sized images of apparently random black-and-white pixels are superimposed, the Wikipedia logo appears.

In this example, the image has been split into two component images. Each component image has a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one ■□, and the other □■. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match: both ■□ or both □■. When these matching pairs are overlapped, they will appear light gray.

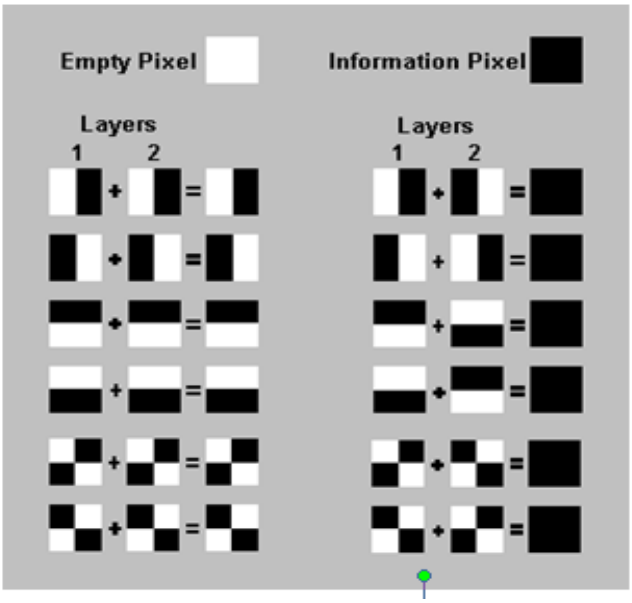
So, when the two component images are superimposed, the original image appears. However, considered by itself, a component image reveals no information about the original image; it is indistinguishable from a random pattern of ■□ / □■ pairs. Moreover, if you have one component image, you can use the shading rules above to produce a counterfeit component image that combines with it to produce any image at all.

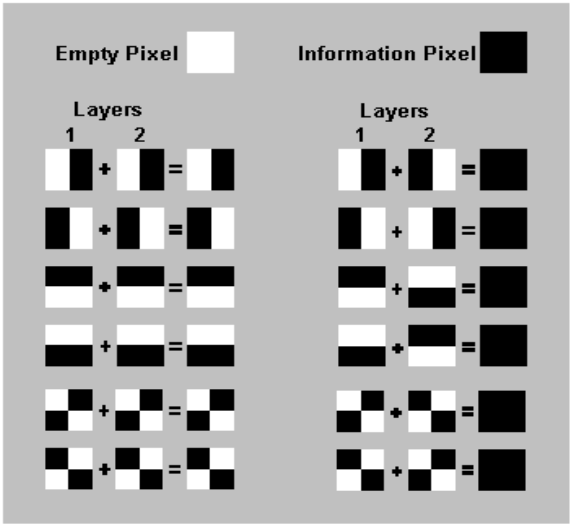
What is Visual Cryptography?

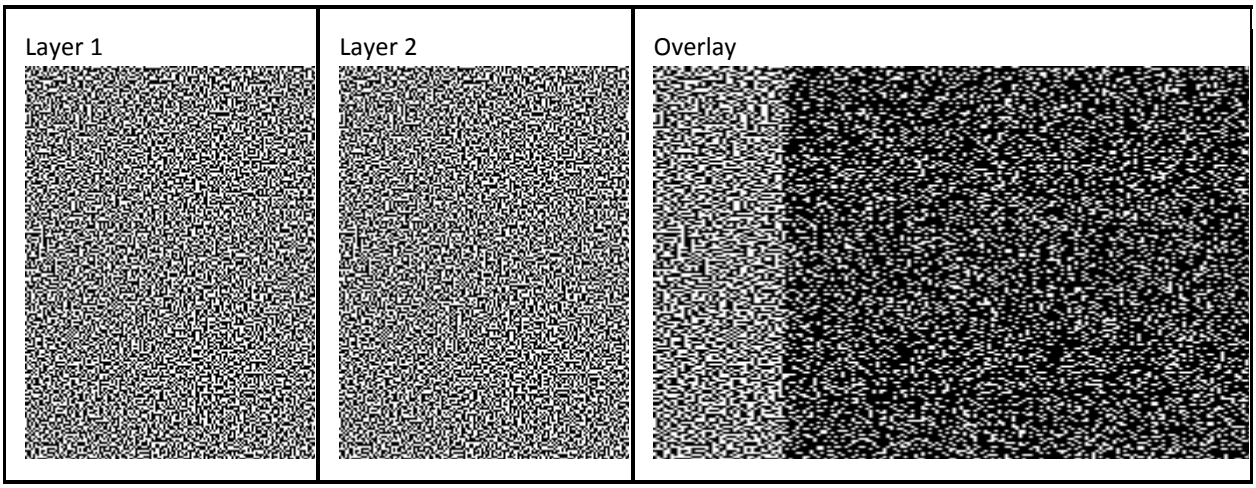
Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

When the random image contains truely random pixels it can be seen as a one-time

pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.







Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table on the right we can see that a pixel, divided into four parts, can have six different states.If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

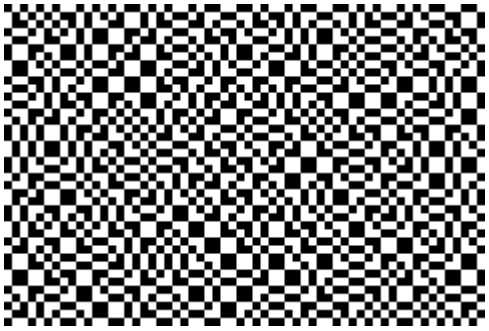
If the pixel states of layer 1 are truly (crypto secure) random, both empty and

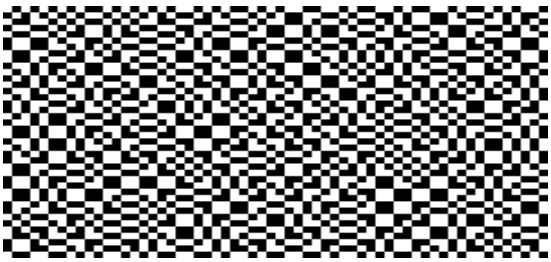
information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand.

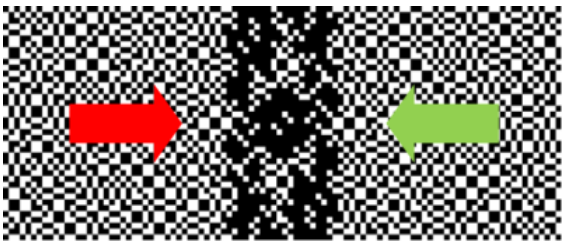
The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

The basis of the technique is the superposition (overlaying) of two semi-transparent layers. Imagine two sheets of transparency covered with a seemingly random collection of black pixels.





Individually, there is no discernable message printed on either one of the sheets. Overlapping them creates addition interference to the light passing through (mathematically the equivalent of performing a Boolean OR operation with the images), but still it just looks like a random collection of pixels.



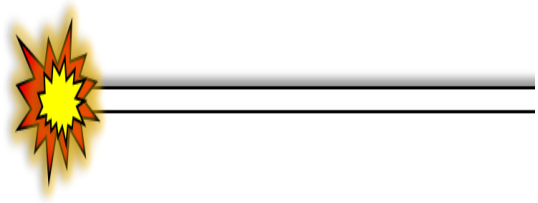
Mysteriously, however, if the two grids are overlaid correctly, at just the right position, a message magically appears!

The patterns are designed to reveal a message.

Demonstration

Let's look at couple of examples of this in action, then we'll describe how the technique works.

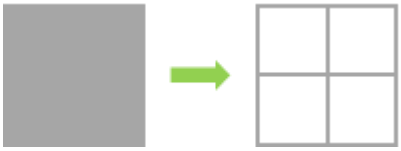
Below you will see two random looking rectangles of dots. One is fixed in the center, and the other you can drag around the canvas. As the rectangles intersect, the images merge. If you align the rectangles perfectly, a hidden message will appear. There are three hidden message to see in this demonstration, once you've decoded one, click on the square button in the bottom left to advance to the next.



To give you feedback, once the images are perfectly aligned, the advance button will go blank with a red border (don't worry, your computer will not self-destruct in five seconds)

How does it work?

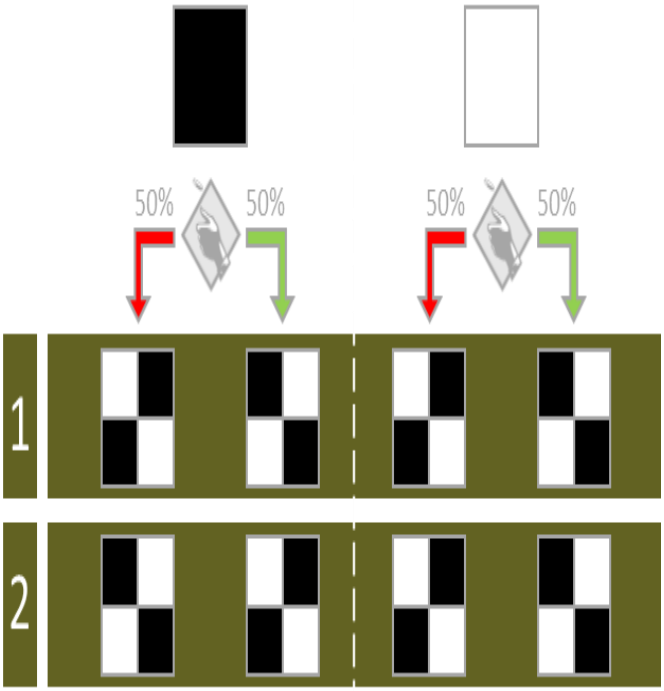
First we take a monochrome image for the source. Pixels in the image are either white or black. To the right is the source for the first example we saw above.



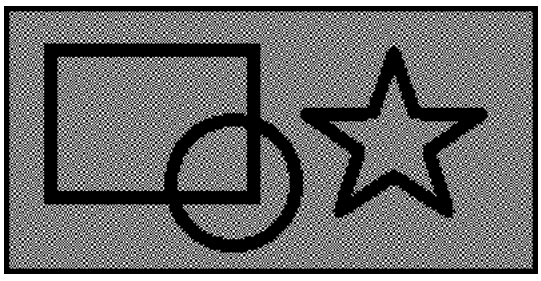
Next we sub-divide each pixel into four smaller subpixels. We need to shade these four subpixels to represent the source image, then subjectively divide them between the two cypher images we are to create.

We need to distribute the shading such that, if you have just one of the cypher images, it is impossible to determine what is on the other cypher image, and thus, impossible to decrypt the image.

What we do is look at the color of each pixel in the original source image. If the original pixel in the image is set (black), we fill in all four sub pixels then distribute them two per cypher layer. We flip a coin to determine which pattern we place on which layer (so that it is random). It does not matter which pair of pixels goes on which layer, when they are combined, all four pixels will be black.



Conversely, if the source image pixel is white, we shade in just two pixels. This time, however, we make sure that the same pixels are shaded on both layers. In this way, when the two cypher images are combined, only two pixels are shaded. As before, we flip a coin to determine which chiral set we go with, and make sure the same image appears on both layers.



Someone who has possession of only one of the cypher images will be able to determine the *(2 x 2)* pattern of each pixel but has no idea if the corresponding pixel cluster on the other image is the same (white space), or opposite (black pixel). Every grid of *(2 x 2)* sub pixels on both layers contains exactly two pixels.

Of course, the two pixels selected do not have to follow checker-board pattern I used above. As long as two are shaded at random, and the rules followed as to whether the same, or complementary, pixels are shaded on the other layer, the system will work.

Here is a short animation of a some of these *(2 x 2)* pixel sub-blocks sliding over each other:

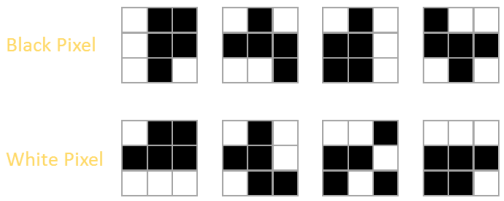
Pretty cool, huh? Well hold on, it gets cooler …

Moni Naor, Adi Shamir, and more people …

The original paper by *Naor* and *Shamir* talks about how to implement this system in a more generic way. For instance, instead of splitting the image into just two cypher texts, why don't we split the image between *n*-cyphertexts; all of which are needed to be combined to reveal the final image? (Or possibly a subset of any *k* images out of these *n*).

If you are interested in reading more, you can find a reprint of the original paper here.

As an example, here are some *(3 x 3)* sub-elements that could be used to distribute an image over four cypher images, all of which are needed to be combined to reveal the secret images:



The top line shows the subpixels used to represent a black pixel in the original images, and the bottom line a white pixel.

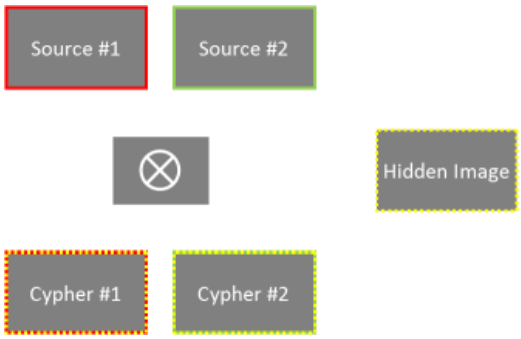
- Any single share contains exactly five black subpixels.
- Any stacked pair contains exactly seven black subpixels.
- Any stacked triplet contains eight black subpixels.

However, when all four in each row are combined, the top row contains *nine* subpixels (all black), whilst the lower row contains only *eight* (allowing light to shine through and creating the contrast necessary to read the image).

You can see from this how the colluding of *any two* or *any three* people is not enough to reveal the secret.

(Mathematically it's possible to do this with eight, not nine, sub-pixels , but there's no easy way to sub divide and pack a square array with eight!)

Deeper down the rabbit hole: *Visual Steganography*



I've done this below. Trust me, you're not going to believe this at first. You're going

to be convinced that there is some 'behind the scenes' script at work that changes the image. I assure you this is not the case. You're still not going to believe me!

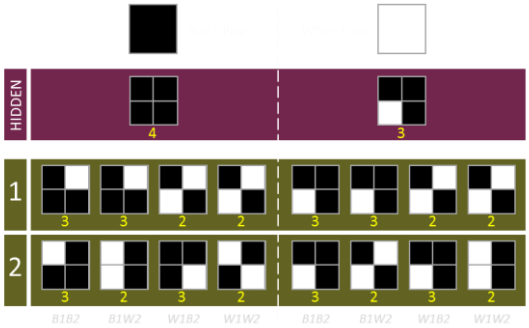
Below, on the left, is my name, encoded from a monochrome image, and also containing partial details of a third hidden image. On the right is the word 'Fish', similarly encoded. Now, drag the right image over to the left image and watch what happens when they overlap perfectly. Wham! How cool is that?

How does this magic work?

The hidden image we are encoding has black pixels and white pixels. As before, we sub divide each pixel into (2 x 2) subpixels. When the two images are combined, we want to represent the black pixels of the hidden image by having all four subpixels black. We'll represent the white pixels has having three subpixels black. This is sufficient contrast for the hidden image to be seen.

For each black or white pixel in the hidden image, there are four possible combinations of black and white pixels of the two source images. For the two source images, we're going to say that any three black subpixels represents black in that source image, and any two pixels represents white.

Examples of all eight permutations of source, image 1 and image 2 are depicted below:



When the hidden image pixel is **BLACK**:

- The combined two cypher images (OR) have to have all four subpixels set.

- When both source images also have a black pixel, this is easy. Both cypher images need to have three out of the four subpixels set. The only constraint is that the missing subpixel is not the same on both layers. One subpixel is randomly selected on the first layer, and one is randomly select from the other three on the second layer.

- When the first image has a black pixel (requiring three subpixels set), and the second image has a white pixel (requiring two

subpixels set), as above, first, a random single subpixel is selected on the black layer to remove. Next two subpixels are randomly selected on the second layer with the constraint that one of the selected subpixels is the same as the gap in the first layer. In this way, when the two are combined, four black subpixels are displayed.

- The opposite happens when the first layer is white, and the second layer is black.

- Finally, if both source pixels are white (requiring just two subpixels set), two subpixels are selected at random on the first layer, and the inverse of this selection used for the second layer.

When the hidden image pixel is **WHITE**:

The combined two cypher images (OR) have to have any three subpixels set.

- When both source images have a black pixel, this is easy. Both cypher images need to have three out of the four subpixels set, and these need to be the same subpixels. Three subpixels are randomly selected and these are set on both of the cypher image layers.

- When the first image has a black pixel (requiring three subpixels set), and the second image has a white pixel (requiring two subpixels set), as above, first, three random subpixels are selected on the first layer. Next one of these three subpixels is randomly selected for removal and this pattern is used on the second layer.

- The opposite happens when the first layer is white, and the second layer is black.

- Finally, if both source pixels are white (requiring two subpixels set), two are selected at random on the first layer, then one of these is duplicated on the second layer, and a second random subpixel is selected on the second layer (from the two white subpixels *not*selected on the first layer). Both layers have two subpixels, and when combined, there are three subpixels visbile.

Other potential uses of the concept

The ability to give an answer, and potentially mask a true answer to a question, tangentially, reminds me of a technique used to get truthful representations in surveys where the subject is potentially embarrassing or where there is incentive to not give a truthful answer.

Imagine you are conducting a survey with the aim of measuring certain characteristics of your audience, and the subject of some of the questions is sensitive (for example, questions about political preference, sexual orientation, whether you have committed fraud, or cheated, or made a mistake that has cost your company thousands of dollars). People might have a motivation to give a non-truthful answers, possible from embarrassment, peer pressure, or fear.

Also, paranoid people might not want to give truthful answers for fear that, even if the survey is anonymous, answers to other questions might be enough to allow an individual to be distinctly identified and thus his answers to the sensitive questions

The solution? Give the people taking your questionnaire a coin. When the question appears e.g. “Have you ever made a mistake that has cost your company thousands of dollars?”, ask the subject to flip a coin. If the coin comes up HEADS, tell the person to answer the question truthfully. If the coin comes up TAILS, tell the person to flip the coin again and if the coin lands HEADS to answer ”Yes” and if the second flip

Any person looking at the survey results and seeing a ”Yes” on an answer will not know if any single person's answer is truthful, or the result of a coin flip. Any person can be free of embarrassment as none of his/her peers will know either.

The law of large numbers, however, will allow a good estimate of the number of people *"Who have made a costly mistake"*, because you’d be able to subtract the number of expected fake *”Yes”* answers,

then scale up the remainder of the answers.

Other articles related to this topic

If you liked this article, you might also like this article about Steganography, and this one about Sharing Secrets.

You can find a complete list of all the articles here. Click here to receive email alerts on new articles.

In the image below you can see how you'd have to handle the sheets. You can also test the images on the source site in my program.

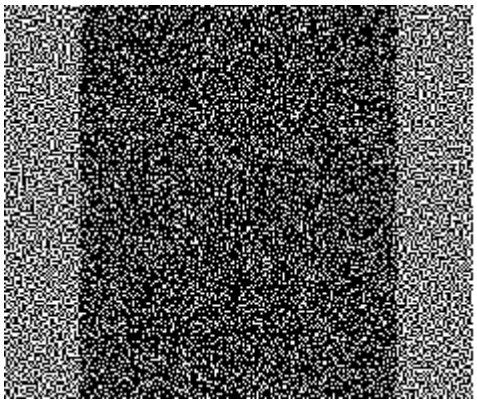


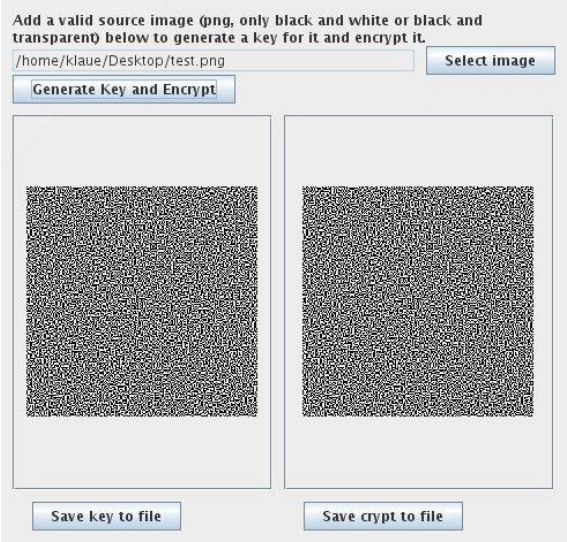
Image Source: Rijmenants, Dirk. Cipher Machines & Cryptology: Visual Cryptography, http://users.telenet.be/d.rijmenants

New in version 2.0 (17.02.2017) is the implementation of Visual Steganography as described in this blog post by datagenetics.com. With Visual Steganography you can hide one picture in two others, see screenshots for an example.

Back to contents

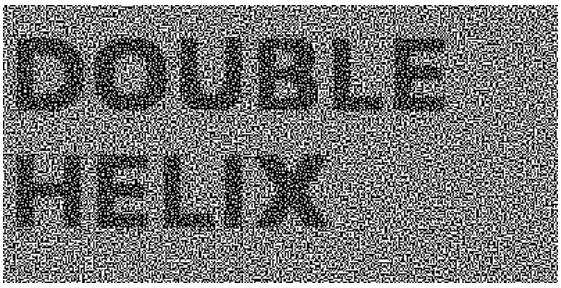
Screenshots

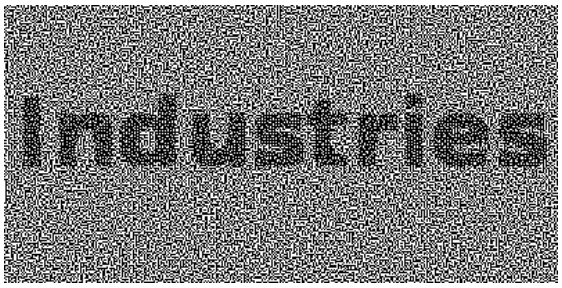
Encryption:

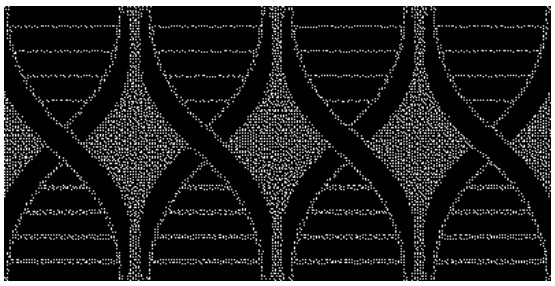


Steganography:

First image Second image Result of overlaying image 1 & 2







Download them and try yourself! Or, if your browser supports that, just drag and drop one over the other - gotta be pixel perfect though!

Back to contents

1.1.1 Features

- Generating a cryptographic secure key
- Encryption of PNG, GIF and JPG images
- Decryption of PNG images
- Hiding an image in two others (Steganography)
- Easy handling

1.1.2 System requirements

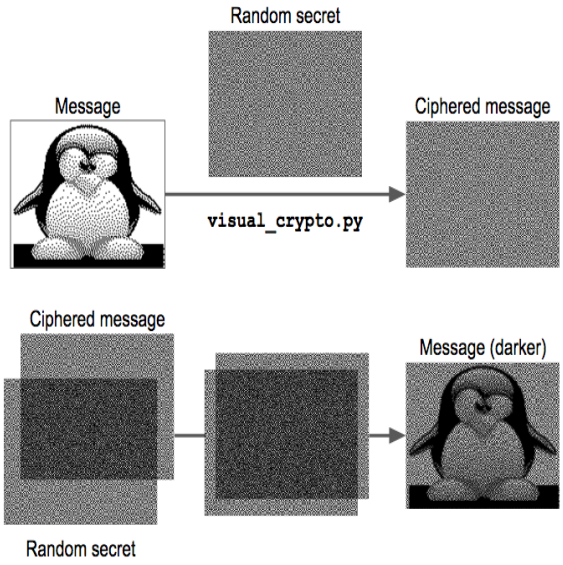
Java2 version 8 or newer. You can check if you have it using this command line command (Windows: Start->run->cmd):

java -version

If you get nothing or if it's telling you that it doesn't know the command "java", you probably don't have java. If you get something, it should look like this:

java version "1.8.0_92"

Java(TM) SE Runtime Environment (build 1.8.0_92-b14)



CHALLENGES

The contrast of the reconstructed image is not maintained. Perfect alingnment of the transperiencies is trablesome. Due to pixel expansion the width of the decoded image is twice as that of the original image. Leads to loss of information due to change in aspect ratio. Additional processing is required for colored images. Its original formulation is restricted only to binary images. For colored images addition proceesing has to be done.

EXAMPLE:

6 Thieves share a bank account. They don't trust one another. The thieves spilt up the for the account in such a way that any 3 or more thieves working together can have to access to account but not<3

RESULT

Visual cryptography is used to encrypt written text/pictures etc in a perfectly secure way. Decoing is done by human visual system without any computation. Method of dividing a serect mogst a group of participants. Each participant get a share of the secret. Sufficient number of shared combined reveals the secret.

Example:

K by n scheme(k,n)

Consider the data D (text/image)divided into n number of shares(D1,D2,……Dn)

K or more shares when overlapped reveals information about the data

K-1 or fever shares when overlapped receives no information about the data.

If k=n then all Participants are required to reconstruct the secret.

CONCLUSION

Among various advantages of visual cryptography scemes is the property that the vcs decoding relies purely on human visual system which leads to a lot of interesting applications in private and public sectors of our society. Visual cryptography is used with short messages therefore giving the crpptanalyst little to work with. Visual cryptography can be used with other data hiding techniques to provide better security. Visual cryptography uses short message public keys can be encrypted using simple method and it proved that security can be attained with even simple encryption schemes.

ACKNOWLEDGMENT

The author is very much grateful to Prof. Ajith Danti, Director and HOD, Department of Master of Computer Application for allowing to do research work in Visual Cryptography. Author is very much grateful to Prof. Sudeep, Assistat professor Department of Master of Computer Application for giving opportunity to do research project.

REFRENCES

I. 1.Moni Naor and Adi Shamir "Visual Cryptography" In Proc. Eurocrypt 94, Perugia, Italy, May 9–12, LNCS 950, Springer Verlag, 1994,1–12.

II. " What are Visual Secret Sharing Schemes"General concept..

Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson, "Visual Cryptography for general access structure", ICALP'96, Italy, 1996

III. Frank Stajano, "Visual Cryptography Kit", Computer Laboratory, University of Cambridge, 1998, http://www.cl.cam.ac.uk/~fms27/vck/

IV. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, "Half tone Visual Cryptography", IEEE Transaction on image processing,vol.15, no.8, 2006.

V. StelvioCimato, Alfredo De Santis, Anna Lisa , Ferrara, Barbara Masucci, "Ideal contrast visual cryptography schemes with reversing", Information Processing Letters, Elsevier.

VI. Jim Cai, "A Short Survey On Visual Cryptography Schemes", 2004.

VII. M.Naor and A.Shamir. "Visual cryptography II: Improving the contrast via the cover base". Theory of Cryptography Library, (96-07), 1996.

VIII. M.Naor and A.Shamir "Visual cryptography, advances in Cryptology". Eurocrypt 94 Proceeding LNCS, 950: 1–12, 1995.

IX. Ch. RatnaBabu, M.Shridhar , Dr. B. RaveendraBabu "Information Hiding in a Gray Scale Image using Pseudo – Randomised Visual Cryptography Algorithm for Visual Information Security", IEEE, 2013.

X. Yicong Zhou, Karen Panetta, SosAganian, "(n, k, p) Gray Code for Image System", IEEE Transaction on Cybernetics, vol.43, No.2, April 2013. Adhikari, A., Sikdar, S.: A new (2,n)-visual threshold scheme for color images. In:Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 148–161.Springer, Heidelberg (2003)

XI. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography forgeneral access structures. Inf. Comput. 129(2), 86–106 (1996)

XII. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended schemes for visual cryptography. Theoret. Comput. Sci. 250(1–2), 143–161 (2001)

XIII. Blundo, C., Cimato, S., De Santis, A.: Visual cryptography schemes with optimal pixel expansion. Theoret. Comput. Sci. 369(1–3), 169–182 (2006)

XIV. Blundo, C., D'Arco, P., De Santis, A., Stinson, D.R.: Contrast optimal threshold visual cryptography schemes. SIAM J. Discrete Math. 16(2), 224–261 (2003) Visual Cryptography 37

XV. Blundo, C., De Santis, A., Stinson, D.R.: On the contrast in visual cryptography schemes. J. Cryptol. 12(4), 261–289 (1999)

XVI. Biham, E., Itzkovitz, A.: Visual cryptography with polarization. In: The Dagstuhl Seminar on cryptography (1997) and Crypto 1998 RUMP Session (1998)

XVII. Chaum, D.: Secret-ballot receipts: true voter-verifiable elections. IEEE Secur. Priv. 38–47 (2004)

XVIII. Chen, T.-H., Lee, Y.-S.: Yet another friendly progressive visual secret sharing scheme. In: 5th International Conference Intelligent Information Hiding and Multimedia Signal Processing, pp. 353–356 (2009)

XIX. Chen, T.-H., Tsao, K.-H.: Visual secret random grids sharing revisited. Pattern Recogn. 42(9), 2203–2217 (2009)

XX. Chen, T.-H., Tsao, K.-H.: Threshold visual secret sharing by random grids. J. Syst. Softw. 84(7), 1197–1208 (2011)

XXI. Cimato, S., De Prisco, R., De Santis, A.: Optimal colored threshold visual cryptography schemes. Des. Codes Crypt. 35, 311–335 (2005)

XXII. Cimato, S., De Prisco, R., De Santis, A.: Probabilistic visual cryptography schemes .Comput. J. 49(1), 97–107 (2006)

XXIII. Cimato, S., De Prisco, R., De Santis, A.: Colored visual cryptography without color

darkening. Theoret. Comput. Sci. 374(1–3), 261–276 (2007)

XXIV. Cimato, S., De Santis, A., Ferrara, A.L., Masucci, B.: Ideal contrast visual cryptography schemes with reversing. Inf. Process. Lett. 93(4), 199–206 (2005)

XXV. Cimato, S., Yang, C.-N.: Visual Cryptography and Secret Image Sharing. CRC Press, Boca Raton (2012). ISBN: 978-1-4398-3721-4

XXVI. D'Arco, P., Prisco, R.: Secure two-party computation: a visual way. In: Padr´o, C. (ed.) ICITS 2013. LNCS, vol. 8317, pp. 18–38. Springer, Heidelberg (2014). doi:10.1007/978-3-319-04268-8 2

XXVII. D'Arco, P., De Prisco, R., De Santis, A.: Measure-independent characterization of contrast optimal visual cryptography schemes. J. Syst. Softw. 95, 89–99 (2014)

XXVIII. D'Arco, P., De Prisco, R., Desmedt, Y.: Private visual share-homomorphic computation and randomness reduction in visual cryptography. In: ICITS 2016, 9–12 August 2016, Tacoma, Washington, USA (2016)

XXIX. De Bonis, A., De Santis, A.: Randomness in secret sharing and visual cryptographyschemes. Theoret. Comput. Sci. 314(3), 351–374 (2004)

XXX. De Prisco, R., De Santis, A.: Cheating immune threshold visual secret sharing.Comput. J. 53(9), 1485–1496 (2009)

XXXI. De Prisco, R., De Santis, A.: Color visual cryptography schemes for black andwhite secret images. Theoret. Comput. Sci. 510(28), 62–86 (2013)

XXXII. De Prisco, R., De Santis, A.: On the relation of random grid and deterministicvisual cryptography. IEEE Trans. Inf. Forensics Secur. 9(4), 653–665 (2014)

XXXIII. Eisen, P.A., Stinson, D.R.: Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. Des. Cods Crypt. 25, 15–61 (2002)

XXXIV. Fang, W.P.: Friendly progressive visual secret sharing. Pattern Recogn. 41(4),1410–1414 (2008)

XXXV. Feng, J.-B., Wu, H.-C., Tsai, C.-S., Chang, Y.-F., Chu, Y.-P.: Visual secret sharing for multiple secrets. Pattern Recogn. 41(12), 3572–3581 (2008)

XXXVI. Hofmeister, T., Krause,M., Simon, H.U.: Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoret. Comput. Sci. 240(2), 471–485 (2000)

XXXVII. Horng, G., Chen, T.-H., Tsai, D.-S.: Cheating in visual cryptography. Des. Codes Crypt. 38(2), 219–236 (2006)

XXXVIII. Hou, Y.-C.: Visual cryptography for color images. Pattern Recognit. 36(7), 1619– 1629 (2003) P. D'Arco and R. De Prisco

XXXIX. Hu, C.-M., Tzeng, W.-G.: Compatible ideal contrast visual cryptography schemes with reversing. In: Zhou, J., Lopez, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 300–313. Springer, Heidelberg (2005). doi:10.1007/11556992 22

XL. Hu, C., Tzeng, W.G.: Cheating prevention in visual cryptography. IEEE Trans. Image Process. 16(1), 36–45 (2007)

XLI. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. 12(6), 377–379 (1987)

XLII. Klein, A., Wessler, M.: Extended visual cryptography schemes. Inf. Comput. 205(5), 716–732 (2007)

XLIII. Koga, H., Yamamoto, H.: Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Trans. Fundam. Electron. Commun. Comput.Sci. 81–A(6), 1262–1269 (1998)

XLIV. Kolesnikov, V.: Gate evaluation secret sharing and secure one-round two-party computation. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 136–155. Springer, Heidelberg (2005). doi:10.1007/11593447 8

XLV. Krause, M., Simon, H.U.: Determining the optimal contrast for secret sharing schemes in visual cryptography. Comb. Probab. Comput. 12(3), 285–299 (2003)

XLVI. Kuhlmann, C., Simon, H.U.: Construction of visual secret sharing schemes with almost optimal contrast. In: 11th ACM-SIAM Symposium on Discrete Algorithms, San Francisco, USA, pp. 262–272 (2000)

XLVII. Lee, K.-H., Chiu, P.-L.: An extended visual cryptography algorithm for general access structures. IEEE Trans. Inf. Forensics Secur. 7(1), 219–229 (2012)

XLVIII. Lee, S.-S., Na, J.-C., Sohn, S.-W., Park, C., Seo, D.-H., Kim, S.-J.: Visual cryptography based on interferometric encryption technique. ETRI J. 24(5), 373–380 (2002)

XLIX. Liu, F., Wua, C., Lin, X.: A new definition of the contrast of visual cryptography scheme. Inf. Process. Lett. 110(7), 241–246 (2010)

L. Liu, F., Wu, C.K.: Optimal XOR based (2,n)-visual cryptography schemes. In: Shi,Y.-Q., Kim, H.J., P´erez-Gonz´alez, F., Yang, C.-N. (eds.) IWDW 2014. LNCS, vol. 9023, pp. 333–349. Springer, Heidelberg (2015)

LI. Lu, S., Manchala, D., Ostrovsky, R.: Visual cryptography on graphs. J. Comb. Optim. 21(1), 47–66 (2011)

LII. Naor, M., Pinkas, B.: Visual authentication and identification. In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 322–336. Springer, Heidelberg (1997). doi:10.1007/BFb0052245

LIII. Naor, M., Shamir, A.: Visual cryptography. In: Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). doi:10.1007/BFb0053419

LIV. Shyu, S.-J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., Chen, K.: Sharing multiple secrets in visual cryptography. Pattern Recogn. 40(12), 3633–3651 (2007)

LV. Stinson, D.: Visual cryptography and threshold schemes. Dr. Dobbs J. (1998). http://www.drdobbs.com/visual-cryptography-threshold-schemes/184410530

LVI. Tulys, P., Hollman, H.D., van Lint, J.H., Tolhuizen, L.: XOR-based visual cryptography schemes. Des. Codes Crypt. 27, 169–186 (2005)

LVII. Verheul, E.R., van Tilborg, H.C.A.: Constructions and properties of k out of n visual secret schemes. Des. Codes Crypt. 11, 179–196 (1997)

LVIII. Viet, D.Q., Kurosawa, K.: Almost ideal contrast visual cryptography with reversing. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 353–365. Springer,Heidelberg (2004). doi:10.1007/978-3-540-24660-2 27

LIX. Yang, C.-N.: New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. 25(4), 481–494 (2004)Visual Cryptography 39