



Visual cryptography: A brief survey

P. Punithavathi & S. Geetha

To cite this article: P. Punithavathi & S. Geetha (2017) Visual cryptography: A brief survey, Information Security Journal: A Global Perspective, 26:6, 305-317, DOI: [10.1080/19393555.2017.1386249](https://doi.org/10.1080/19393555.2017.1386249)

To link to this article: <https://doi.org/10.1080/19393555.2017.1386249>



Published online: 15 Nov 2017.



Submit your article to this journal [↗](#)



Article views: 295



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)



Visual cryptography: A brief survey

P. Punithavathi  and S. Geetha

Research scholar, School of Computing Science and Engineering, VIT University, Chennai, India

ABSTRACT

Visual cryptography is an emerging technology to address the concerns regarding privacy of images. It is a powerful technique combining both the impeccable ciphers and secret sharing in cryptography with that of the raster graphics. Visual cryptography divides the secret image into shares or shadows during encryption. The term “visual” in visual cryptography stands for the fact that during decryption phase, a user can perceive the recovered secret with his/her visual system, without the intervention of machines. Various visual cryptography techniques have been discussed extensively in this survey. The metrics used to analyse the effectiveness of visual cryptography techniques have been briefed. The significant applications of visual cryptography have also been summarized in the survey.

KEYWORDS

Visual cryptography; shares; pixel-expansion; contrast loss; image-level biometric template protection

Introduction

Visual Cryptography (VC) is a paradigm in which a secret image is converted into two or more meaningless, non-identical shares, without using any encryption keys. The hidden secret can be revealed only when the shares are stacked together. VC is a desirable scheme as it embodies both the scheme of perfect secrecy and a very simple mechanism for recovering the secret. VC provides robust security to the secret image. This makes VC suitable for highly sensitive applications like biometric authentication (Ross & Othman, 2011), secure electronic ballots (Chaum, 2004), safe online banking (Roy & Venkateswaran, 2014), digital watermarking (Tai & Chang, 2004), security against Denial-of-Service (DoS) attacks in WiMax authentication system (Altaf, Sirhindi, & Ahmed, 2008), etc.

This survey is organized as follows: Taxonomy of VC (Section 2), Applications (Section 3), Metrics to analyse the quality of reconstructed secret image in VC (Section 4), Future direction (Section 5), and research issues (Section 6). A broad discussion including the current state-of-the-art approaches to visual cryptography, classifications and applications of VC

has been given along with brief concluding remarks (Section 7).

Taxonomy of visual cryptography

Visual cryptography for binary image

The secret image is divided into two or more shares in VC using a share generation technique. The taxonomy of VC (shown in Figure 1) discussed in this section is based on the type of the input image i.e. binary, grayscale and color image, and based on the logical operation used during share recovery.

Pixel-based visual cryptography

The pixel-based visual cryptography was pioneered by (Naor & Shamir, 1995). The basic model is extended into a visual variant of k out of n i.e., (k, n) secret sharing problem. Given the secret image, n shares are generated such that the secret image is visible only if any k number of shares are stacked together (where k is less than or equal to n). The image cannot be reconstructed if fewer than k shares are stacked together. The shares are collections of m black and white sub-pixels corresponding to the pixels in the secret image. The contrast of the image was enhanced using a cover base in (Naor & Shamir, 1997).

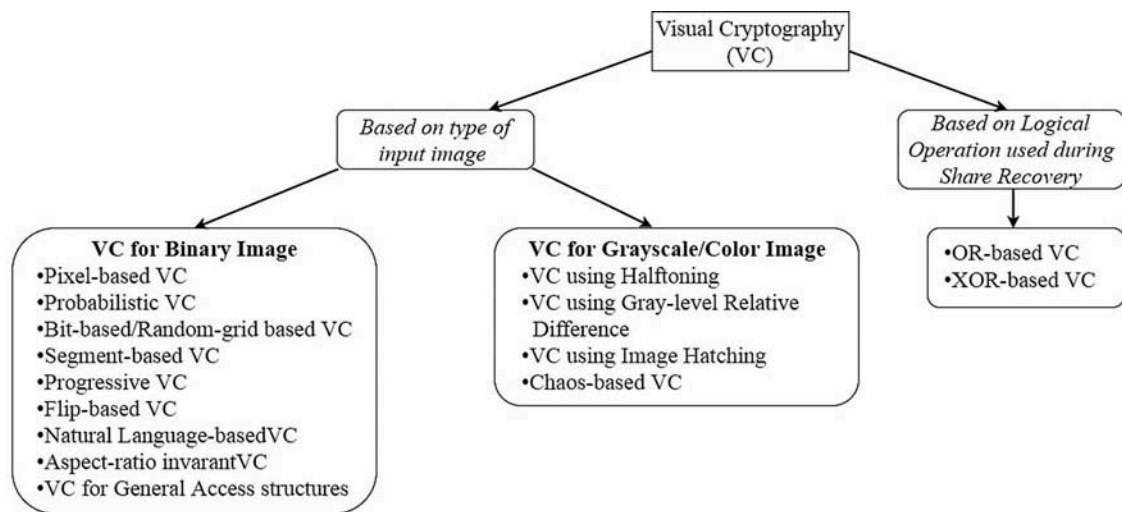


Figure 1. Taxonomy of visual cryptography.

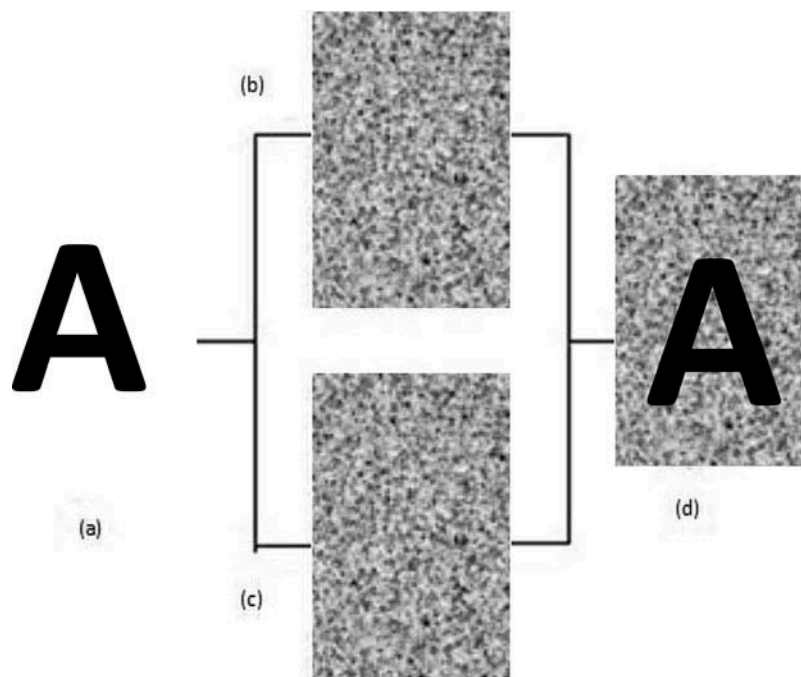


Figure 2. Pixel-based VC proposed by Naor & Shamir, (Naor & Shamir, 1997). (1) Secret image (b) Share 1 (c) Share 2 (d) Recovered Image

















The scheme can be explained using (2,2) model as shown in Figure 2. Each secret pixel is divided into two sub-pixels. Two combination matrices (C_0 and C_1) are generated representing white and black pixels respectively. C_0 contains combinations of matrices which each share should contain while encrypting a white pixel. Similarly C_1 contains combinations of matrices which each share should contain while encrypting a black pixel. It can be understood from Table 1 that the sub-pixels which represent a white pixel in the

secret image are identical while the sub-pixels representing a black pixel are non-identical.

The shares 1 and 2, shown in Figure 2, are generated in the following manner:

- If a pixel in the secret image is white, then same pattern of sub-pixels is selected for both shares. (This implies that to share a white pixel, one of the matrices is selected randomly from C_0 for each share).

Table 1. Coding table of share blocks.

Pixel in secret image	Share1	Share2	Pixel in restored image
			
			
			
			

- If a pixel in the secret image is black, then complementary pair of patterns of sub-pixels is selected for both shares. (This implies that to share a black pixel, one of the matrices is selected randomly from $C1$ for each share).

It is clear that any single share is a random choice of two white and two black sub-pixels with respect to a particular pixel in secret image. This gives the impression of being medium gray. When the shares are stacked together, the result is either medium gray (representing white) or completely black (representing black).

The ORed ' m ' vector, V_0 corresponding to $C0$ is (1,0) or (0,1) because of the process of selection of the same sub-pixel pattern. The ORed ' m ' vector V_1 corresponding to $C1$ is always (1,1) because of the process of selection of the complementary sub-pixel patterns. The Hamming weight of any two shares of a white pixel is '1' and the Hamming weight of any two shares of a black pixel is '2'. Let us assume that the value of a predetermined threshold ' d ' to be '1' (since the value of d must be $1 \leq d \leq m$). This implies that the pixels with Hamming weight of '1' is interpreted as white and

'2' is interpreted as black, by the human visual system.

Each share comprises of several sub-pixel patterns which are built up of two white and two black pixels. The individual shares give no clue of whether a specific pixel is black or white in the secret image. Hence it is impractical to decrypt the share even by applying enormous computation.

Since the white pixels in secret image become 50% black and 50% white during the selection of sub-pixel pattern, the contrast of the recovered image becomes poor.

Extended visual cryptography. The concept of extended visual cryptography was first coined by (Droste, 2001). However the work of (Ateniese, Blundo, Santis, & Stinson, 2001) was remarkable. This was entirely dependent on the pixel-based visual cryptography proposed by (Naor & Shamir, 1995).

The entire set of shares is divided into two sets – one is qualifying set (which reveals the secret when superimposed) and the other one is forbidden set (which never reveals the secret even if superimposed together). Apart from this each share must be meaningful i.e. there should be a cover image for each secret as shown in Figure 3.

Multiple image visual cryptography. A multiple image visual cryptography was proposed by (Wu & Chen, 1998). It is capable of hiding more than one secret within the shares as shown in Figure 4. While recovering, the shares are superimposed on each other to reveal first secret. One of the shares is rotated to particular angle and then again superimposed with other share to reveal the second secret. Another technique for securing multiple images has been proposed in (Wu & Chang, 2005). In order to increase the ease of rotation, Wu and Chang proposed that the shares are circular in shape. Since these are extended versions of pixel-based visual cryptography, the pixel-expansion and contrast loss are still persistent in these techniques.

Probabilistic visual cryptography

Probabilistic VC is an approach targeted towards suppressing pixel expansion problem arising out of

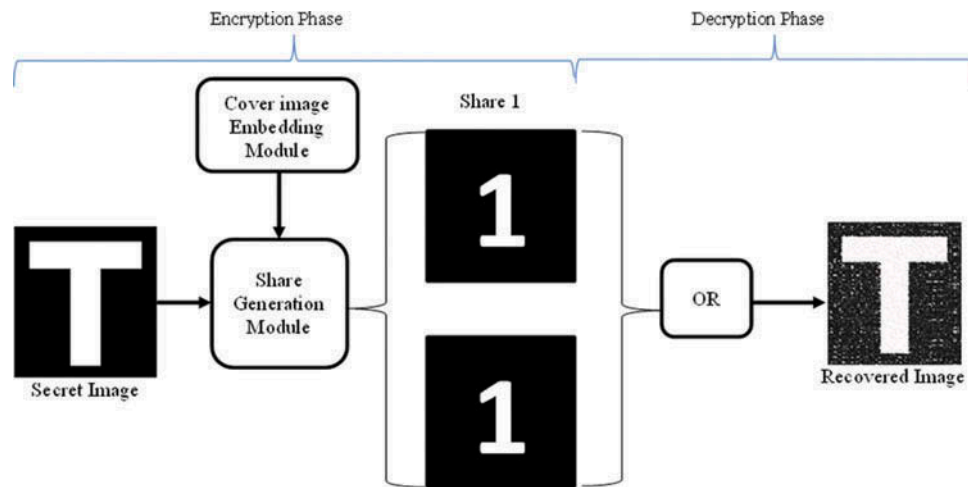


Figure 3. Extended VC proposed by (Ateniese et al., 2001).

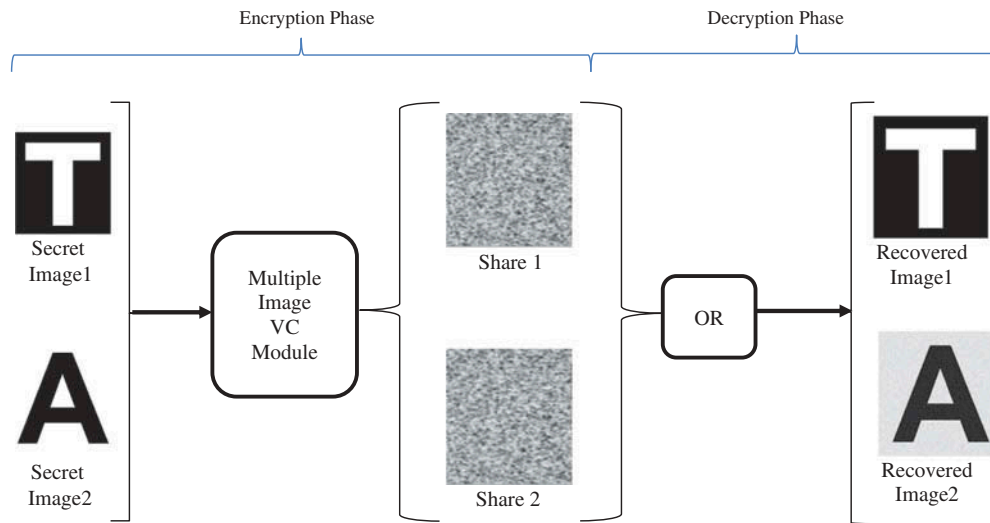


Figure 4. Multiple image VC.

pixel-based VC. The probabilistic approach by (Yang, 2004) has no pixel expansion, and the secret image is reconstructed based on a certain probability ratio. The contrast of the recovered secret is however same as that of the pixel-based VC. Probabilistic VC techniques were also designed by (Cimato, De Prisco, & De Santis, 2005) (Yang, Wu, & Wang, 2014) and (De Prisco & De Santis, 2014)

Bit-based/random grid-based visual cryptography

The random grid-based visual cryptography was pioneered by (Kafri & Keren, 1987). They suggested that secret is hidden into random grid. The random grid is a transparency which is comprised

of a two-dimensional array of pixels which may be black or white, and the choice between them is made by a coin-flip procedure. There is no association between the values of the pixels in the array. Since the size of the random grid is same as that of the input secret, the shares do not suffer from pixel expansion. Several other visual cryptography techniques dependent on the random-grid, were also proposed by (Shyu, 2007), (Chen, Tsao, & Wei, 2008) and (Lin, Lin, & Chen, 2014). (Shyu, Huang, Lee, Wang, & Chen, 2007), extended the multi-secret VC scheme of (Wu & Chang, 2005) from single rotation to numerous rotations so that they could encode 'n' images into 2 transparencies. An attempt was made to

adapt the circular-shares to embed two sets of confidential messages into different angles of the shares (Wu & Chang, 2005). This overcomes the limited choice of rotating angle and increases security.

Extended visual cryptography. The extended VC can be employed using random grids similar to that of the extended VC using pixel-based approach. An extended VC scheme proposed in (Shyu, 2009) is comprised of hiding a secret within multiple random-grids, making the scheme attractive towards practical applications. An improved extended visual cryptography has been proposed in (Hou, Wei, & Lin, 2014) which has better visual quality of recovered image. The shares generated using this method are random grids which have different cover images on them.

Multiple image visual cryptography. Multiple image VC has been implemented using random-grids in (Chen et al., 2008). Two secrets were hidden within two random grids. One of the secrets can be recovered by superimposing the shares directly while the other share is recovered by rotating the random grids and then superimposing them. A kind of multiple image VC using random grid can be seen in (Wang & Lee, 2010). The secrets can be revealed by stacking the shares. At the same time the folding-up of a share up can disclose some identification patterns. Hence both secret information and the designated identification patterns can be recognized by naked eye without any computation.

Segment-based visual cryptography

The segment-based VC (Borchert, 2007) is based on seven-segment display pattern unlike pixel-based traditional VC. It is used to hide messages comprising numbers. The advantage of the segment-based VC is that it may be uncomplicated to adjust the secret images and that the symbols are potentially easier to recognize for the human eye. The seven-segment display is comprised of seven bars (three horizontal and four vertical) which are arranged like a digit '8'. Every digit from 0, ..., 9 can be represented just by highlighting the selective segments. The seven-segment

display is comprised of seven bars (three horizontal and four vertical) which are arranged like a digit '8'. Every digit from 0, ..., 9 can be represented just by highlighting the selective segments.

The principle of pixel-based VC is applied to the segment-based visual cryptography. Assume that every segment S_n ('=' or '|') in the seven segment display model, is comprised of two parallel segments S_{n1} and S_{n2} . ('—' or '|'), which are very close to each other but do not intersect each other.

Progressive visual cryptography

The progressive VC is a simple technique to recover the secret image gradually by superimposing more and more shares. If few pieces of shares are available, we could get only an outline of the secret; by increasing the number of shares that are stacked, the entire details of the secret information could be exposed, progressively. Different techniques of progressive VC were proposed by (Fang W. P., 2007), (Fang & Lin, 2006), (Chen & Lin, 2005), and (Jin, Yan, & Kankanhalli, 2005).

Flip-based visual cryptography

The flip-based visual cryptography scheme (Lin, Chen, & Lin, 2010) encodes two secret images into two dual-purpose shares. The first secret image is revealed by stacking two transparencies. The second secret is revealed by flipping one of the two shares and then stacking it with the other share. The proposed scheme is also proved to have conditionally optimal contrast and enhanced security.

Natural language-based visual cryptography

The concept of the natural language letter-based visual cryptography (Lin, Yang, Lai, & Lin, 2013) introduces the concept of using letters or alphabets or numbers during share generation. The pixels are replaced by letters in the share images. Moreover the shares become meaningful because of the appearance of letters on them, and escape suspicion by an adversary.

Aspect-ratio invariant visual cryptography

The aspect ratio of an image is defined as the proportional relationship between height and

width of the image. It is denoted as two numbers separated by a colon e.g. 15:3. The change in aspect ratio during encryption phase of VC affects the visual perception of the secret image. Several VC techniques with pixel-based operations have been introduced in (Yang & Chen, 2005) and (Yang & Chen, 2006) to avoid change in the aspect ratio. An aspect-ratio invariant VC has also been discussed in (Yang, Chen, Shih, & Kim, 2013) which uses image filtering and resizing operations.

Visual cryptography for general access structures

General access structures can be used to specify the combinations of shares during decryption phase rather than number of shares as seen in (Ateniese, Blundo, De Santis, & Stinson, 1996). For instance, consider a firm comprising one owner, one supervisor and two employees. The level of decryption has to be set such that the employees can never access the secret. The supervisor can recover the secret only with the employees. The owner can recover the secret with any of his colleagues. Hence the VC has to be treated as a special case of general access structure.

Visual cryptography for grayscale and color images

The VC techniques discussed so far are applicable to binary images only. These VC techniques cannot be applied directly on grayscale or color image. Hence a pre-processing technique is required to

convert the grayscale image/color image to be suitable for the application of VC. This pre-processing technique is called as halftoning technique.

Halftoning is a reprographic technique that simulates continuous tone imagery through the use of dots, varying either in size or in spacing, thus generating a gradient-like effect. The continuous tone imagery contains an infinite range of colors or grays. The halftone process reduces visual reproductions to an image that is turned out with only one color of ink, in dots of differing size or spacing. These tiny halftone dots are blended into smooth tones by the human visual system. The grayscale or color images are first halftoned, and then subjected to VC as shown in Figure 5. Several halftoning techniques described in (Ulichney, 1987) are shown been tabulated in Figure 6.

Several approaches for implementing VC on halftoned images have been proposed in (Hou, 2003), (Hou & Tu, 2005), (Shyu, 2006), (Zhou, Arce, & Di Crescenzo, 2006), (Wang, Arce, & Di Crescenzo, 2009) (Cimato, De Prisco, & De Santis, 2011), (Askari, Moloney, & Heys, 2012), (Askari, Heys, & Moloney, 2013), (Askari, Heys, & Moloney, 2014), and (Ou, Ye, & Sun, 2015). However halftoning itself is a reduction process. Hence the halftoned images subjected to VC will be surely affected by contrast loss.

Apart from halftoning, Moire's pattern (Desmedt & Van Le, 2000), and graylevel relative difference (Blundo, De Santis, & Naor, 2000) can also be used for applying VC on grayscale images. Similarly, image

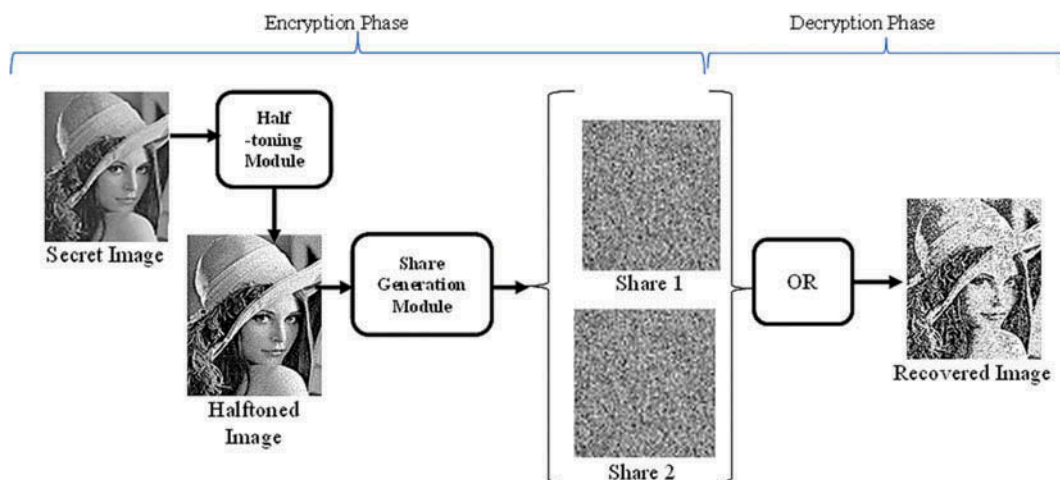


Figure 5. VC for grayscale image using halftoning technique.

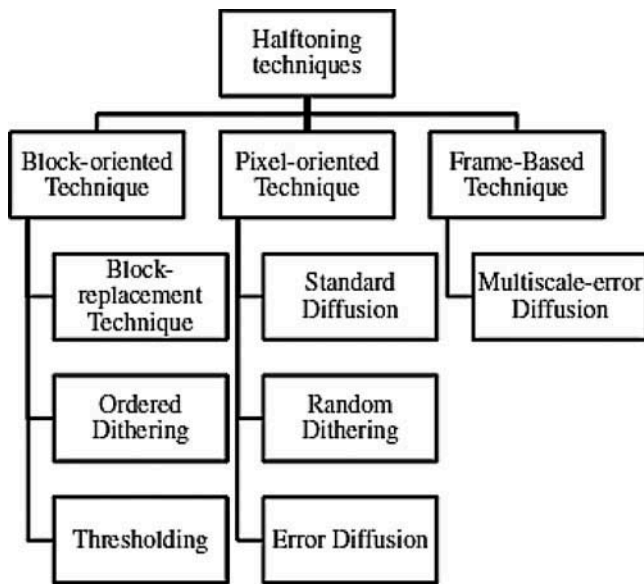


Figure 6. Types of halftoning techniques.

hatching technique (Weir, Yan, & Kankanhalli, 2012) can also be used to apply VC on color images.

Chaos-based visual cryptography

Apart from usual approach of processing the pixel values (based on algorithm) to generate shares, a new idea has been incorporated by (Huynh, Bharanitharan, & Chang, 2015). Along with the pixel values, the pixel positions are also employed to generate the shares using chaotic mapping. A Quadri-directional searching algorithm has been employed to exploit the four-dimensional search strategy on Sudoku table while constructing the shares and as well as while reconstructing secret image.

The approach is divided into two sub-processes: the share construction phase, and the secret image recovering and cover reconstructing phase. The pixels in secret image are at first converted into a base-9 numerical system to obtain a group of digits. While mapping this group of digits to the reference Sudoku table, there are four directions from the mapped value: North-West, North-East, South-East and South-West which contains all the pixels located in the upper-left corner, upper-right corner, bottom-right corner, and bottom-left corner, respectively. The main advantage of the method is that a grayscale secret image can be processed directly

without any halftoning technique. Thereby the contrast loss due to halftoning technique has been cut-off. This avoids pixel-expansion problem.

Another chaos-based visual cryptography has been proposed in (Goswami, Mukherjee, & Ghoshal, 2017). It restricts unauthorized tampering of digital/digitized documents during wireless communication by exploiting the properties of discrete wavelet transformation.

Based on logical operation used during share recovery

The decryption process is very simple in VC. The shares are stacked or superimposed one on the other in order to reconstruct the secret from the share. Logical operations like 'OR' or 'XOR' operations can be utilized during recovery operation. Based on this, the VC system is classified into OR-based VC and XOR-based VC.

Or-based VC

The shares are superimposed to reconstruct the secret image again. This operation is eventually equivalent to logical OR operation. The VC schemes using logical OR operation to recover the secret image are called OR-based VC. The pixel-based VC proposed in (Naor & Shamir, 1995) and (Ateniese et al., 2001) are best examples of OR-based VC.

Xor-based VC

When numerous shares are superimposed, the reconstructed secret has a lower visual quality because the recovered image becomes darker. On the other hand, XOR-based VC (Tuyls, Hollmann, Van Lint, & Tolhuizen, 2005), (Wang, Zhang, Ma, & Li, 2007) and (Wu & Sun, 2013) is a significant branch of VC which can reconstruct the secret without darkening the background when more shares are utilized. XOR-based VC system has good color, contrast and resolution properties compared to OR-based VC systems.

Applications of VC

VC suitable for highly sensitive applications like biometric authentication (Ross & Othman, 2011), secure electronic ballots (Chaum, 2004), safe

online banking (Roy & Venkateswaran, 2014) digital watermarking (Tai & Chang, 2004), security against DoS attacks in WiMax authentication system (Altaf et al., 2008), etc.

Visual cryptography for biometric privacy

A visual cryptography technique implemented in (Ross & Othman, 2011) can be effectively used to secure the biometrics. Two types of schemes were introduced. One was basic visual cryptography for fingerprint and iris, and the other one was graylevel extended visual cryptography for face. The basic visual cryptography scheme, illustrated in Figure 7, generates shares corresponding to the input biometric trait – fingerprint or iris. These shares are stored in different databases. The graylevel extended visual cryptography generates shares from a set of public host database, corresponding to input biometric trait – face. When these shares are superimposed, the hidden biometric template can be extracted and matched with the input probe. The matching rates were promising.

However the drawback with the method is that it requires two different databases to store the shares since they cannot be stored on the same database for security reasons.

Another algorithm has been proposed in (Askari et al., 2014) which is based on balanced block replacement technique of halftoning methodology. Using this method a grayscale image is converted into halftone image without any pixel-expansion. Hence the shares also overcome the problems due to pixel-expansion. This property suits the usage of this algorithm into biometric template security technique.

VC for security against dos attacks in wimax authentication system

VC has been successfully employed for security against DoS attacks in WiMax authentication system (Altaf et al., 2008). The base station allots most of its resources to evaluate certificates of the parties involved in authentication procedure. This becomes an overhead. Hence a simple visual secret sharing scheme has been employed during pre-authentication scenario to avoid DoS attacks caused by the

large number of rouge requests. A simple XOR operation is used to check the validity of requesting sub-station and base station both, thus providing mutual authentication scheme. Hence DoS attacks can be avoided along with an additional layer of security in the WiMAX authentication.

Safe online banking using VC

A safe online payment system has been proposed in (Roy & Venkateswaran, 2014) using steganography and VC. This promotes a secure payment system for the customers during online shopping. A system proposed in (Lu et al., 2017) uses a combination of VC and quick response code for safe mobile banking.

Secure electronic ballot using VC

VC (Chaum, 2004) has been employed to verify the election outcome even if the situations when all the election systems and records are compromised. The system preserves ballot secrecy economically, while improving access, robustness, etc.

Secure multiparty computation using VC

The process of designing secure protocols that can be used without the assistance of a computer and without any prior knowledge of cryptography, is interesting. The protocols enjoying these features could be useful in a variety of settings where computers cannot be used or where people feel uncomfortable to interact with a computer. D'Arco and De Prisco in (D'Arco & De Prisco, 2013) and (D'Arco & De Prisco, 2016) have proposed a technique which employs VC in multiparty computation environment has been discussed.

Metrics to analyse the quality of VC algorithm

Table 2 Shows several VC techniques and a comparative analysis of these techniques using metrics like contrast loss, pixel expansion, etc. The quality of the reconstructed image in VC can be assessed using the following metrics:

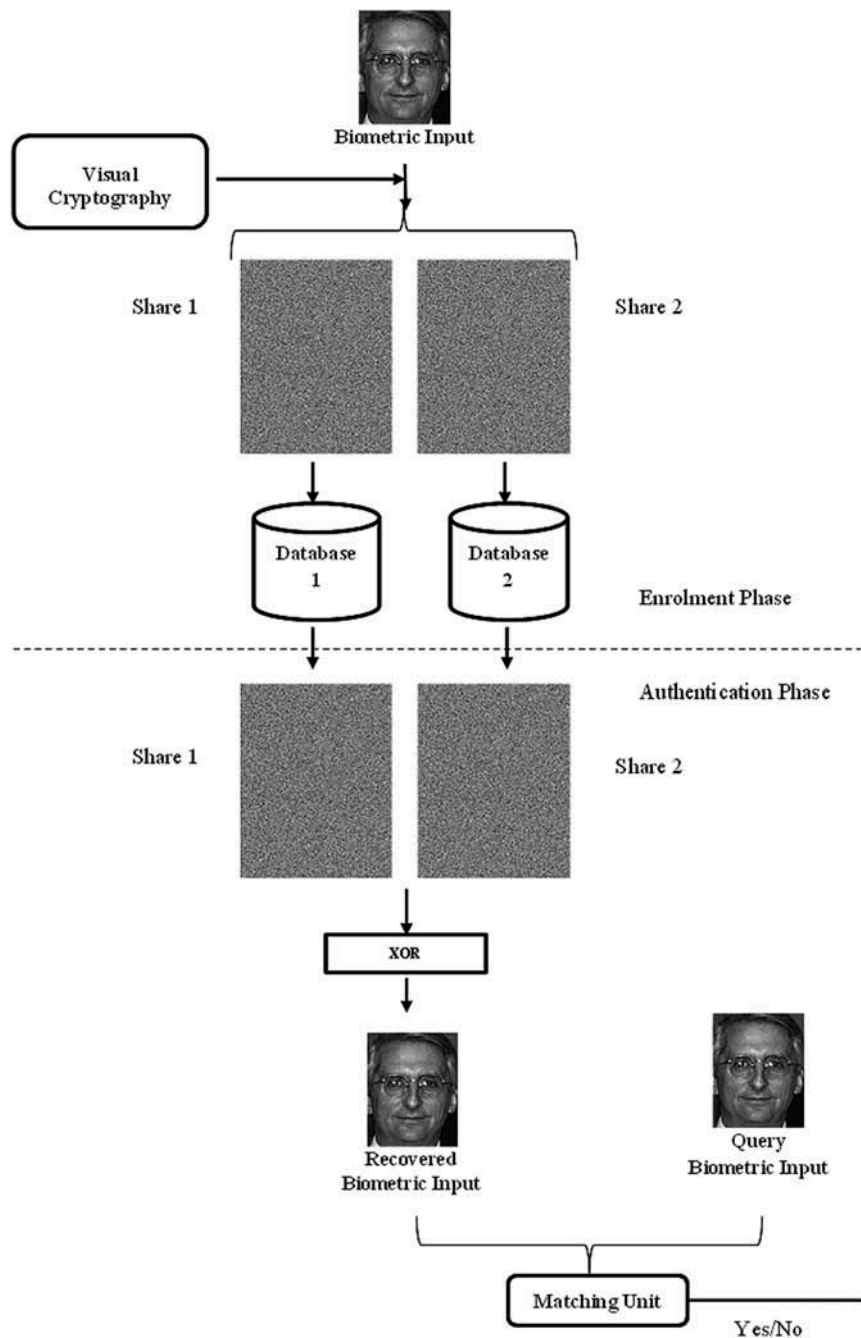


Figure 7. Biometric authentication scheme proposed in (Ross & Othman, 2011).

Contrast loss

The pixels in secret image are converted into combination of black and white subpixels in pixel-based VC. Similarly in bit-based approach the random-grid are transparencies with random bits representing black and white pixels of the secret image. The secret image is reconstructed again just by superimposing the shares together. During this process, the black pixels in shares

representing the white pixels of the secret image cause contrast loss. A VC scheme with very low contrast loss is desirable.

Pixel expansion

The size of the shares generated using pixel-based VC is proportional to the number of sub-pixels used to represent each pixel in secret image. This

Table 2. Comparison of various visual cryptography schemes.

Author(s)	Technique	No. of secrets	No. of shares	Pixel Expansion	Contrast loss
Kafri & Keren, 1987	Bit-based VC	1	2	nil	$\frac{1}{2}$ or $\frac{1}{4}$
(Naor & Shamir, 1995)	Pixel-based VC	1	2	m	1/m
Desmedt & Van Le, 2000	Moire's pattern	1	2		
Blundo et al., 2000	Graylevel relative difference	1	2	255.m	1/(255.m)
Ateniese et al., 2001	Extended VC	1	2	m	1/m
(Hou, 2003)	VC for color image	2	2	m	1/m
Yang, 2004	Probabilistic VC	1	2	nil	1/2
Tuyls et al., 2005	XOR-based VC	2	2	m	minimum
Wu & Chang, 2005	Multiple image VC	2	2	m	1/m
Jin et al., 2005	Progressive VC	1	n	m	1/m
Borchert, 2007	Segment-based VC	1	2	-	-
Lin et al., 2010	Flip-base VC	2	2	nil	minimum
Weir et al., 2012	Image hatching	1	2	m	1/m
Lin et al., 2013	Natural language letter-based VC	1	2	-	-
Askari et al., 2014	VC for grayscale image using halftoning technique (Block-replacement)	2	2	nil	minimum
Huynh et al., 2015	Chaotic VC	1	2	nil	nil

*am represents number of sub-pixels

is referred to as pixel expansion. Pixel expansion affects data transmission and storage. The pixel-expansion can be minimized by using bit-based VC approach. A VC scheme with very low pixel expansion is desirable.

Security level/level of pixel distortion

The security level of the VC scheme represents the strength of the encryption phase. Each share generated during encryption phase, should never reveal any information about the secret image individually, unless superimposed. The security level of the encrypted share can be measured using the metrics like number of changing pixel rate and unified average change -in-intensity.

Time complexity of algorithm

The main objective of any VC algorithm is that it should not be with high time complexity during decryption i.e. decryption should be performed without intervention of machines. The secret image has to be reconstructed for direct perception of human eyes.

Future direction

The images reconstructed using visual cryptography, mostly suffer from pixel expansion and contrast loss. Though visual cryptography seems to be

simple, these flaws appear to be a threat in bringing out the entire magnificence of visual cryptography. While using VC for securing secret information in sensitive applications like biometric authentication, one must be careful about the matching performance. The contrast loss must be minimized or eradicated to achieve such a high accuracy.

The major concern due to pixel expansion is requirement of storage space. Each share may be bigger than the secret thereby requiring more storage space. A VC scheme utilized must be efficient such that it brings about very low contrast loss and pixel expansion.

Since there are two shares generated from single secret, there must be two different databases to store these shares. In order to reduce storage difficulties, one of the shares can be handed over to the user in the form of tokens, cards, etc. This share must be submitted during decryption for bringing out the secret hidden within the shares. Hence a VC scheme with reduced pixel expansion and low contrast loss is desirable in securing the sensitive information. It is necessary that further research be conducted in this direction.

Conclusion

Various types of visual cryptography (VC) schemes have been surveyed. The importance of VC schemes

to enhance the integrity and security of secret information have also been discussed. This may be a key to open the research in using VC for securing secret information even in cloud environment. A tradeoff is required in some schemes depending on the size of the shares along with the number of secrets which may be concealed. It becomes vital to ensure that the base images completely disappear and a clear secret is recovered which could be another high quality image.

Acknowledgment

Authors are thankful to the Management of VIT University-Chennai Campus. The first author has been supported by Visvesvaraya Ph. D. Scheme funded by Media Lab Asia, Ministry of Electronics and Information Technology, Government of India.

Notes on contributors

Punithavathi received Bachelor of Engineering in 2007, and M. Tech in 2014. She has achieved University Rank for M. Tech. She has served as Editor in publishing industry for four years. She also has four years of teaching experience. She is pursuing Ph. D. at VIT University, Chennai, presently.

Geetha received the B.E., from the Madurai Kamaraj University, M.E., and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai, in 2000, 2004 and 2011 respectively. She has 14+ years of teaching experience. Currently, she is serving as a Professor at School of Computing Science and Engineering at VIT-University, Chennai Campus. She has published many papers in reputed IEEE/ACM/Springer International Conferences and refereed Journals. She joins the review committee and editorial advisory board of journals like IEEE Transactions on Information Forensics and Security and IEEE Transactions on Image Processing, Springer Multimedia Tools and Security, Elsevier – Information Sciences. She was an editor for the Indian Conference proceedings of ICCIIS 2007 and RISES-2013. Her research interests include multimedia security, intrusion detection systems, machine learning paradigms and information forensics. She has delivered many expert lectures, keynote addresses in international and national conferences. She is a recipient of University Rank and Academic Excellence Award in B.E. and M.E. in 2000 and 2004 respectively. She is also a pride recipient of the “Best Academic Researcher Award 2013”, “Best Professor Award 2014” of ASDF Global Awards.

ORCID

P. Punithavathi  <http://orcid.org/0000-0002-8322-8312>

References

- Altaf, A., Sirhindi, R., & Ahmed, A. (2008). *A novel approach against DoS attacks in WiMAX authentication using visual cryptography*. Second International Conference on Emerging Security Information, Systems and Technologies (pp. 238–242), Cap Esterel.
- Askari, N., Heys, H. M., & Moloney, C. R. (2013). *An extended visual cryptography scheme without pixel expansion for halftone images*. 26th Annual IEEE Canadian Conference on Electrical and Computer Engineering, Canada. (pp. 1–6).
- Askari, N., Heys, H. M., & Moloney, C. R. (2014). Novel visual cryptography schemes without pixel expansion for Halftone images. *Canadian Journal of Electrical and Computer Engineering*, 37(3), 168–177. doi:10.1109/CJECE.2014.2333419
- Askari, N., Moloney, C., & Heys, H. M. (2012). *A novel visual secret sharing scheme without image size expansion*. 25th IEEE Canadian Conference on Electrical & Computer Engineering, Canada. (pp. 1–4).
- Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual cryptography for general access structures. *Information and Computation*, 129(2), 86–106. doi:10.1006/inco.1996.0076
- Ateniese, G., Blundo, C., Santis, A., & Stinson, D. (2001). Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250(1–2), 143–161. doi:10.1016/S0304-3975(99)00127-9
- Blundo, C., De Santis, A., & Naor, M. (2000). Visual cryptography for grey level images. *Information Processing Letters*, 75(6), 255–259. doi:10.1016/S0020-0190(00)00108-3
- Borchert, B. (2007). *Segment-based visual cryptography*. Wilhelm-Schickard-Institut für Informatik, Universität Tübingen, Germany.
- Chaum, D. (2004). Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy Magazine*, 38–47. doi:10.1109/MSECP.2004.1264852
- Chen, S., & Lin, J. (2005). Fault-tolerant and progressive transmission of images. *Pattern Recognition*, 2466–2471. doi:10.1016/j.patcog.2005.04.002
- Chen, T. H., Tsao, K. H., & Wei, K. C. (2008, November). *Multiple-image encryption by rotating random grids*. In Intelligent Systems Design and Applications, 2008. ISDA'08. Eighth International Conference on (Vol. 3, pp. 252–256). Taiwan: IEEE.
- Cimato, S., De Prisco, R., & De Santis, A. (2005). Probabilistic visual cryptography schemes. *The Computer Journal*, 49(1), 97–107. doi:10.1093/comjnl/bxh152
- Cimato, S., De Prisco, R., & De Santis, A. (2011). Visual cryptography for color images. *Visual Cryptography and Secret Image Sharing*, 32–56.
- D'Arco, P., & De Prisco, R. (2013, November). Secure two-party computation: A visual way. In *International Conference on Information Theoretic Security*, (pp. 18–38). Singapore: Springer.

- D'Arco, P., & De Prisco, R. (2016). Secure computation without computers. *Theoretical Computer Science*, 651, 11–36. doi:[10.1016/j.tcs.2016.08.003](https://doi.org/10.1016/j.tcs.2016.08.003)
- De Prisco, R., & De Santis, A. (2014). On the relation of random grid and deterministic Visual cryptography. *IEEE Transactions on Information Forensics and Security*, 9(4), 653–665. doi:[10.1109/TIFS.2014.2305574](https://doi.org/10.1109/TIFS.2014.2305574)
- Desmedt, Y., & Van Le, T. (2000). *Moire cryptography*. 7th ACM conference on Computer and communications security (pp. 116–124), Greece.
- Droste, S. (2001). New results on visual cryptography. *Advances in Cryptology — CRYPTO '96 Lecture Notes in Computer Science*, 1109, 401–415.
- Fang, W., & Lin, J. (2006). Progressive viewing and sharing of sensitive images. *Pattern Recognition and Image Analysis*, 16(4), 632–636. doi:[10.1134/S1054661806040080](https://doi.org/10.1134/S1054661806040080)
- Fang, W. P. (2007). *Multi-layer progressive secret image sharing*. Seventh WSEAS International Conference on Signal Processing, Computational Geometry & Artificial Vision (pp. 112–116), Greece.
- Goswami, A., Mukherjee, R., & Ghoshal, N. (2017). Chaotic visual cryptography based digitized document authentication. *Wireless Personal Communications*, 96(3): 1–21.
- Hou, Y. (2003). Visual cryptography for color images. *Pattern Recognition*, 36(7), 1619–1629. doi:[10.1016/S0031-3203\(02\)00258-3](https://doi.org/10.1016/S0031-3203(02)00258-3)
- Hou, Y. C., & Tu, S. F. (2005). A visual cryptographic technique for chromatic images using multi-pixel encoding method. *Journal of Research and Practice in Information Technology*, 37(2), 179–192.
- Hou, Y. C., Wei, S. C., & Lin, C. Y. (2014). Random-grid-based visual cryptography schemes. *IEEE Transactions on Circuits and Systems for Video Technology*, 24(5), 733–744. doi:[10.1109/TCSVT.2013.2280097](https://doi.org/10.1109/TCSVT.2013.2280097)
- Huynh, N., Bharanitharan, K., & Chang, C. (2015). Quadri-directional searching algorithm for secret image sharing using meaningful shadows. *Journal of Visual Communication and Image Representation*, 28, 105–112. doi:[10.1016/j.jvcir.2015.01.011](https://doi.org/10.1016/j.jvcir.2015.01.011)
- Jin, D., Yan, W. Q., & Kankanhalli, M. S. (2005). Progressive color visual cryptography. *Journal of Electronic Imaging*, 14(3), 033019–033019. doi:[10.1117/1.1993625](https://doi.org/10.1117/1.1993625)
- Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. *Optics Letters*, 12(6), 377. doi:[10.1364/OL.12.000377](https://doi.org/10.1364/OL.12.000377)
- Lin, H. C., Yang, C. N., Lai, C. S., & Lin, H. T. (2013). Natural language letter based visual cryptography scheme. *Journal of Visual Communication and Image Representation*, 24(3), 318–331. doi:[10.1016/j.jvcir.2013.01.003](https://doi.org/10.1016/j.jvcir.2013.01.003)
- Lin, K., Lin, C., & Chen, T. (2014). Distortionless visual multi-secret sharing based on random grid. *Information Sciences*, 288(1), 330–346. doi:[10.1016/j.ins.2014.07.016](https://doi.org/10.1016/j.ins.2014.07.016)
- Lin, S. J., Chen, S. K., & Lin, J. C. (2010). Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. *Journal of Visual Communication and Image Representation*, 21(8), 900–916. doi:[10.1016/j.jvcir.2010.08.006](https://doi.org/10.1016/j.jvcir.2010.08.006)
- Lu, J., Yang, Z., Li, L., Yuan, W., Li, L., & Chang, C. C. (2017). Multiple schemes for mobile payment authentication using QR code and visual cryptography. *Mobile Information Systems*. doi:[10.1155/2017/4356038](https://doi.org/10.1155/2017/4356038)
- Naor, M., & Shamir, A. (1995). Visual cryptography. *Advances in Cryptology — EUROCRYPT'94 Lecture Notes in Computer Science*, 950(1), 1–12.
- Naor, M., & Shamir, A. (1997). Visual cryptography II: Improving the contrast via the cover base. *Security Protocols Lecture Notes in Computer Science*, 1189, 197–202.
- Ou, D., Ye, L., & Sun, W. (2015). User-friendly secret image sharing scheme with verification ability based on block truncation coding and error diffusion. *Journal of Visual Communication and Image Representation*, 46–60. doi:[10.1016/j.jvcir.2015.01.017](https://doi.org/10.1016/j.jvcir.2015.01.017)
- Ross, A., & Othman, A. (2011). Visual cryptography for biometric privacy. *IEEE Transactions on Information Forensics and Security*, 6(1), 70–81. doi:[10.1109/TIFS.2010.2097252](https://doi.org/10.1109/TIFS.2010.2097252)
- Roy, S., & Venkateswaran, P. (2014). *Online payment system using steganography and visual cryptography*. IEEE Students' Conference on Electrical, Electronics and Computer Science (pp. 1–5), India.
- Shyu, S. (2006). Efficient visual secret sharing scheme for color images. *Pattern Recognition*, 36(5), 866–880. doi:[10.1016/j.patcog.2005.06.010](https://doi.org/10.1016/j.patcog.2005.06.010)
- Shyu, S. (2007). Image encryption by random grids. *Pattern Recognition*, 40(3), 1014–1031. doi:[10.1016/j.patcog.2006.02.025](https://doi.org/10.1016/j.patcog.2006.02.025)
- Shyu, S. (2009). Image encryption by multiple random grids. *Pattern Recognition*, 42(7), 1582–1596. doi:[10.1016/j.patcog.2008.08.023](https://doi.org/10.1016/j.patcog.2008.08.023)
- Shyu, S., Huang, S., Lee, Y., Wang, R., & Chen, K. (2007). Sharing multiple secrets in visual cryptography. *Pattern Recognition*, 40(12), 3633–3651. doi:[10.1016/j.patcog.2007.03.012](https://doi.org/10.1016/j.patcog.2007.03.012)
- Tai, G., & Chang, L. (2004). Visual cryptography for digital watermarking in still images. *Advances in Multimedia Information Processing - PCM 2004 Lecture Notes in Computer Science*, 50–57.
- Tuyls, P., Hollmann, H. D., Van Lint, J. H., & Tolhuizen, L. M. (2005). XOR-based visual cryptography schemes. *Designs, Codes and Cryptography*, 169–186. doi:[10.1007/s10623-004-3816-4](https://doi.org/10.1007/s10623-004-3816-4)
- Ulichney, R. (1987). *Digital halftoning*. England: MIT Press. ISBN: 0-262-21009-6.
- Wang, D., Zhang, L., Ma, N., & Li, X. (2007). Two secret sharing schemes based on Boolean operations. *Pattern Recognition*, 40(10), 2776–2785. doi:[10.1016/j.patcog.2006.11.018](https://doi.org/10.1016/j.patcog.2006.11.018)
- Wang, R. Z., & Lee, Y. T. (2010). Visual cryptography by random grids with identifiable shares. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 4(5), 965.
- Wang, Z., Arce, G. R., & Di Crescenzo, G. (2009). Halftone visual cryptography via error diffusion. *IEEE Transactions*

- on *Information Forensics and Security*, 4(3), 383–396. doi:[10.1109/TIFS.2009.2024721](https://doi.org/10.1109/TIFS.2009.2024721)
- Weir, J., Yan, W., & Kankanhalli, M. S. (2012). Image hatching for visual cryptography. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 8(2S): 32.
- Wu, C., & Chen, L. (1998). *Study on visual cryptography. Master Thesis, nstitute of Computer and Information Science*. National Chiao Tung University, Taiwan, R.O.C.
- Wu, H., & Chang, C. (2005). Sharing visual multi-secrets using circle shares. *Computer Standards & Interfaces*, 28(1), 123–135. doi:[10.1016/j.csi.2004.12.006](https://doi.org/10.1016/j.csi.2004.12.006)
- Wu, X., & Sun, W. (2013). Generalized random grid and its applications in visual cryptography. *IEEE Transactions on Information Forensics and Security*, 8(9), 1541–1553. doi:[10.1109/TIFS.2013.2274955](https://doi.org/10.1109/TIFS.2013.2274955)
- Yang, C. N. (2004). New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4), 481–494. doi:[10.1016/j.patrec.2003.12.011](https://doi.org/10.1016/j.patrec.2003.12.011)
- Yang, C. N., Chen, P. W., Shih, H. W., & Kim, C. (2013). Aspect ratio invariant visual cryptography by image filtering and resizing. *Personal and Ubiquitous Computing*, 17(5), 843–850. doi:[10.1007/s00779-012-0535-0](https://doi.org/10.1007/s00779-012-0535-0)
- Yang, C. N., & Chen, T. S. (2005). Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. *Pattern Recognition Letters*, 26(2), 193–206. doi:[10.1016/j.patrec.2004.08.025](https://doi.org/10.1016/j.patrec.2004.08.025)
- Yang, C. N., & Chen, T. S. (2006). Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. *Pattern Recognition*, 39(7), 1300–1314. doi:[10.1016/j.patcog.2006.01.013](https://doi.org/10.1016/j.patcog.2006.01.013)
- Yang, C. N., Wu, C. C., & Wang, D. S. (2014). A discussion on the relationship between probabilistic visual cryptography and random grid. *Information Sciences*, 278, 141–173. doi:[10.1016/j.ins.2014.03.033](https://doi.org/10.1016/j.ins.2014.03.033)
- Zhou, Z., Arce, G. R., & Di Crescenzo, G. (2006). Halftone visual cryptography. *IEEE Transactions on Image Processing*, 2441–2453. doi:[10.1109/TIP.2006.875249](https://doi.org/10.1109/TIP.2006.875249)