Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 14, no. 2, February 2018, pp. 334-340
DOI: 10.23940/ijpe.18.02.p14.334340

A Visual Cryptography Scheme-Based DNA Microarrays

Xuncai Zhang, Zheng Zhou, Yangyang Jiao, Ying Niu*, Yanfeng Wang

School of Electrics and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou, 450002, China

Abstract

Visual cryptography is a cryptographic technique that allows visual information to be encrypted in such a way that the decryption can be performed by humans. The power of DNA molecule comes from its memory capacity and parallel processing. In this article, a visual encryption algorithm based on DNA microarrays is proposed, which successfully integrates the advantages of the algorithm in information security with the natural advantages of modern biotechnology. The algorithm converts plaintext into QR code and then uses the visual encryption scheme to encrypt the QR code image. It combines with DNA microarray technology to achieve information encryption and decryption. Security analysis shows that this algorithm has high security.

Keywords: visual cryptography; DNA microarray; DNA sequences; probe; QR code

(Submitted on November 1, 2017; Revised on December 15, 2017; Accepted on January 25, 2018)

1. Introduction

Visual encryption technology is an interesting visual secret-sharing mechanism proposed by Naor and Shamir [15]. The secret sharing and digital image are combined based on the threshold secret-sharing information. The black and white pixels in each share are randomly distributed by encoding the secret images into several shared images by pixel points. Due to the theoretical security of visual cryptography and the simplicity of information recovery, it has been widely used in the field of group participation or control [4,23].

Since visual cryptography was put forward in 1994, scholars have conducted extensive and in-depth research on program improvement [1,22], program optimization and program application [2,6]. This work further optimized the performance of visual cryptographic schemes and enriched the connotation of visual cryptography. Additionally, the development of visual cryptography was greatly promoted [3,8,19].

After more than 20 years of continuous enrichment and development, visual cryptography has developed from the initial (2, 2) threshold scheme into a relatively perfect research direction for a theoretical system [11]. However, in the scheme of visual cryptography sharing, the expansion of pixels reduces the contrast of restored images, and the shared carrier also restricts the practical application of the visual cryptography [5].

The high storage density, high parallelism and the natural advantage of the ultra-low energy consumption of the DNA molecule [24,17] make its potential in the field of storage and computing fully exploited. DNA molecular computing has an unique data storage and computing mechanism that could solve traditionally difficult problems [10,21] with a new perspective, while also providing new opportunities for information security [12,20]. DNA microarray (DNA chip) technology belongs to the category of biological chip technology. It is a large-scale integrated solid-phase hybridization, and it integrates oligonucleotide probes on a solid-phase support that can be synthesized in-situ; alternatively, a large number of prepared DNA probes can be immobilized on the support surface in an orderly manner using microscopic printing. Then, the labeled samples are hybridized with oligonucleotide probes to obtain genetic information from the samples by detecting the hybridization signals produced by the analysis. Therefore, DNA chip technology has been extremely helpful for the

* Corresponding author.
E-mail address: niuying@zzuli.edu.cn

efficient and rapid detection of genetic information. Because of the high integration of DNA chips, there is no effective technique for precise and efficient sequencing of specially designed cryptographic chips. An attacker could not recover plaintext by reading the encrypted chip directly. Therefore, people have begun to explore the application of DNA chips in the field of cryptography [16].

Combined with the advantages of DNA microarray, a visual encryption algorithm based on DNA microarrays is proposed in this paper. The first step is to convert the plaintext into a QR code. Then, the visual encryption scheme is used to encrypt the QR code image. Finally, the receiver uses a key chip and bio-experimental techniques to restore plaintext images hidden in the cipher text chip and its complement chain, which further increases the security of the secret.

2. Visual encryption technology and DNA microarray

2.1. Visual encryption technology

For the sake of description, this paper adopts the (2, 2) threshold scheme, which is the most basic secret sharing scheme of visual cryptography. The (2,2) threshold scheme is to divide each pixel into two or four pixels; if a certain pixel is white, select the segmentation rules using the rows 'A' or 'B' in Figure 1(a) with equal probability. If share '1' is used as the key part in A, then share '2' in row A is used as the cipher text information part, and the position of the second part of the pixel information is unified with the position of the pixel in the original image. Similarly, for a black pixel, the corresponding pixel component is determined by the rule for 'C' or 'D' with equal probability. If the original pixel is black, its decomposition into two parts is still two black sub-pixels. If the original pixel is white, the two parts are decomposed into half white and half black pixels. However, the black and white pixels in the original image can be identified by the visual system after overlapping. Of course, the original image can also be recovered by computer processing. In this way, a pixel in the original image is extended to two sub-pixels, so the area of the shared copy is two times that of the original image. Because of randomness, the black or white pixels in the original image are encrypted into black and white sub-pixels in the shared copies. As a result, it is impossible to obtain any information about the original image from any shared copies.

Figure 1(b) shows the process of decomposing and extracting an image. First, the image to be transmitted is decomposed into Share '1' and Share '2,' which are two picture components. The two components alone seem to be a random collection of black and white pixels, and the independent acquisition of either side of the extraction of information is useless. But if the two translucent layers are stacked together, mathematically, the Boolean operation will be performed for each pixel, and the original image will appear. After such processing, the two images are combined into one, the contrast is reduced to half the size of the original image, the black part of the original picture is still shown as black after decoding, and the white part is displayed in halftone gray. But, the original pattern can still be displayed clearly in the overlapping pattern.

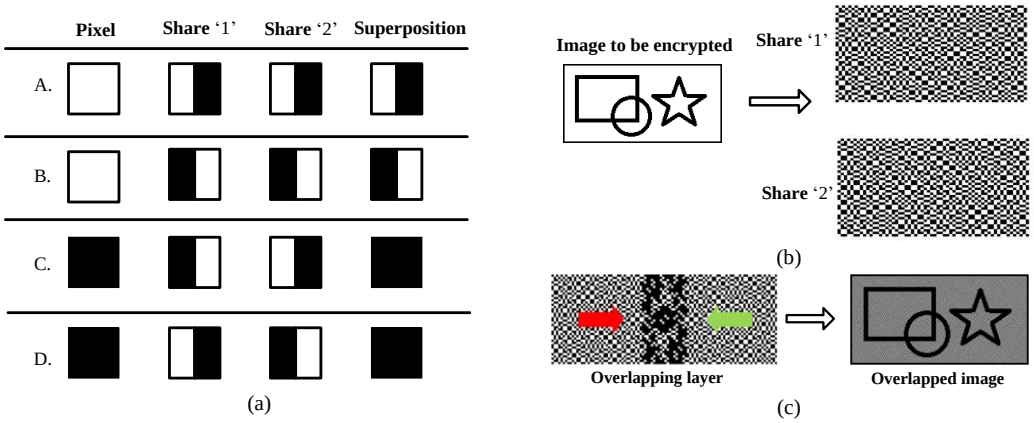


Figure 1. Schematic diagram of visual encryption technology: (a) encryption rules; (b) image decomposition; and (c) image extraction.

2.2. DNA microarray

DNA microarray technology is an emerging field that combines the flexible application of the cutting-edge technology from the life sciences, chemistry, microelectronics technology, laser confocal technology, DNA synthesis, fluorescence labeling probe hybridization, and statistics; DNA microarray technology was developed in the United States of America by Affymetrix, Inc., in San Francisco at the end of 1996 [9,13]. Its technical strategy is to use a large number of single-stranded

DNA fragments as probes, using micro-etching technology or piezoelectric printing technology to solidify the surface of the support object according to a certain rule. Then, the sample is measured according to the principle of complementary base pairing from a PCR reaction. An imaging system is then used to observe fluorescence signals, so as to quickly conduct a series of gene-related studies.

The preparation of DNA chips includes five main steps: the construction of chip array, preparation of the hybridization sample, hybridization reaction between the array and sample, signal detection and analysis of the results. The solid phase supports the production of gene chips that are solid materials, such as silicon chips, glass and porcelain, and others that are film materials, such as polypropylene film, nylon film and nitrocellulose membranes. The types of chip preparation are generally divided into in situ synthesis and direct point-like two major categories. Oligonucleotides are more suitable for in-situ synthesis, with photolithography and piezoelectric printing as two approaches. The direct point sample method is simple for the use of large fragments of DNA without reagents. A computer silicon chip is often used as solid-phase support for general gene chips. Each point on the chip contains 10-12 moles of probe, and the lattice density is higher than 400/cm^2. The probe can add a single strand of DNA to the end of a section of fluorescent markers, and the sequence is known. After the hybridization reaction, the redundant chain, which does not participate in the reaction, is washed away; its complementary chain is retained. Finally, through laser confocal fluorescence detection or the CCD image scanning, qualitative and quantitative analysis is conducted, which produces massive information in a short time. In addition, electronic chips with multiple micro-electrodes, three-dimensional chips that can be simultaneously amplified and detected, and flow-through chips, such as grid-like micro-channels, have been widely used.

3. Encryption method design

The QR code is a black-and-white graphic that is distributed according to certain rules on a plane (two-dimensional surface) by a specific geometry, and utilizes the concept of a ‘0’ and ‘1’ bit stream using the logic of a computer. Black denotes binary ‘1’, and white means binary ‘0’, so the QR code is a key to recording information; we can easily convert text, character and picture information into QR codes.

This scheme is a one-time pad encryption algorithm. This algorithm introduces DNA chip and QR code technology into the visual encryption algorithm. Compared with the original visual encryption algorithm, it can be said that the addition of DNA chip makes the algorithm's confidentiality much higher than the general algorithm. The algorithm mainly involves the encryption of the sender Alice and the extraction of the receiver Bob. The main idea is as follows. Before the encryption, Alice picked a gene chip that randomly labeled the fluorescence of several positions and sent it to Bob in a safe way. Alice pre-processes the image to be encrypted, artificially synthesizes the corresponding DNA sequences according to the gene chip to determine the cipher text DNA sequences, and adds a fluorescent label at the end of the corresponding sequences, according to the encrypted content. The cipher text sequences are prepared by mixing into a physically similar redundant sequences solution and delivered to Bob in a public manner. Bob receives a mixed solution containing the cipher text sequences, hybridizes them with the DNA chip, then flushes the gene chip and observes the fluorescence on the chip, which expresses the binary ‘1’ and ‘0’ according to the fluorescence intensity of the DNA chip. With the aid of image processing software, the cipher text image is recovered, and the information transmitted by Alice is obtained. For this scheme, the key is a randomly selected gene chip, which is the image to be encrypted, and the cipher text is the DNA sequences in the mixed DNA solution received by Bob.

3.1. Scheme design

Definition: Assume that the sender is Alice and the receiver is Bob, and they both agree on a security key as MK. Alice uses MK to convert the plaintext m into cipher text c through the encryption process E, that is, $E(m)=c$. Bob receives cipher text c, and uses MK and cipher text c for the decryption process D to obtain plaintext m, namely, $D(c)=\mathrm{E}(c)^{-1}=m$.The overall scheme of the system is as follows:

Key generation. An encryption key is a specific set of probes, and the corresponding complementary probes are processed (fluorescent tags) as decryption keys. Alice can select probes from existing biological experiments as encryption keys, or she can design her own encryption key through experiments. The decryption key is passed to Bob via a secure path. To further improve safety, a redundant chain is prepared, and the physics of the similar redundant chain of the decryption chain is synthetically reconstructed to enhance the concealment of the decryption key chain. Several redundant chains can be selected and attached with the same type of fluorescent markings to the end.

Encryption. First, the plaintext information is converted into a QR code. According to the visual encryption rule in Figure 1(a), secret information sharing is realized, and two shared copies are generated. Then, the DNA chip and key are

designed for each share, and the DNA chip is cipher text. In the absence of the decryption key, the attacker cannot determine the information represented by each bit in the chip, so it is difficult to obtain plaintext information from the DNA chip. The encryption process is shown in Figure 2.

Decryption. The receiver uses the decryption key to hybridize with the corresponding DNA chip to obtain the hybridization signal, using a confocal laser scanning microscope (CLSM) to scan the hybrid chip point by point, line by line, and side by side rapidly. Then, the signal is processed by the computer, and the information in the QR code is obtained by combining the processed image, which is then converted into plain text information through third-party software. The decryption process is shown in Figure 2.

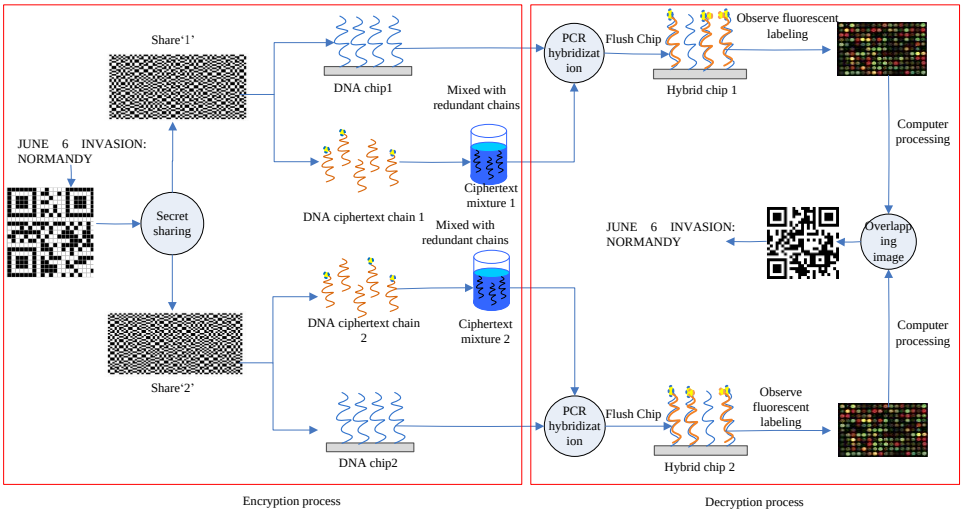


Figure 2. Schematic diagram of the encryption and decryption process.

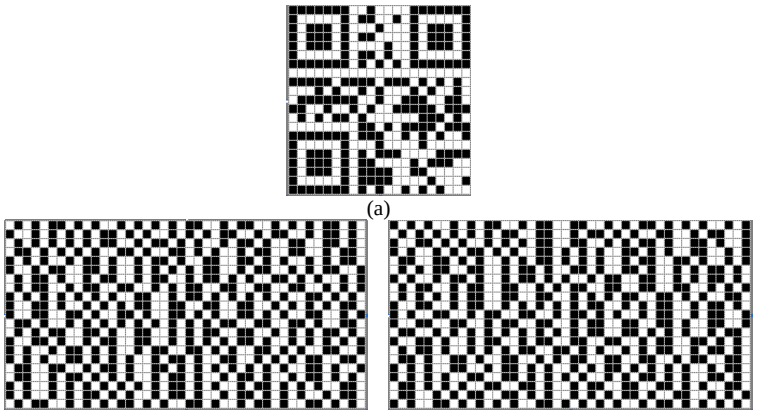
3.2. Simulation and experiment

An example is used to demonstrate the implementation of the scheme, which involves two parts: the sending and receiving end. Suppose that the plaintext to be encrypted is "JUNE 6 INVASION: NORMANDY", and the steps are as follows:

(1) **Key generation**. The generated key is first synthesized by a collection of probes that are known and are different from each other, and this set is ordered on a DNA chip. The target probe sets are then synthesized. All the candidate probes (unlabeled fluorescence) on the DNA chip are used as set α, and all the target probes (labeled fluorescence) in the DNA solution are used as set β. The probe in set α contains two subsets alpha α_0 and α_1. Subset α_0 refers to a DNA probe (represents the binary number 0) that can hybridize with a probe in set β, and the subset α_1 is a DNA probe (represents the binary number 1) that cannot hybridize with a probe in set β. Reasonable criteria are chosen, according to the hybridization results and hybridization conditions, to select the probe [14]. The standard in this paper refers to the strength of the fluorescence intensity; according to the fluorescence intensity in the experiment, the contents of the points on the chip in the set α are selected reasonably. We use only one fluorescent marker in this scheme, and of course we can use two types of fluorescence. The probe set α is used as the encryption key, and the probe set β and the experimental conditions are used as the decryption key. To enhance the concealment of the decryption key, multiple redundant probes are selected as the set γ, and the same types of fluorescent tags are attached at the trailing end, together with set β. The probes in set γ do not hybridize with the probes in set α. It is notable that the total number of pixels of the plaintext to be transmitted is restricted by the number of key probes. This example is used only to describe the process, and the set of probes can be expanded according to the actual situation.

(2) **Encryption**. The plaintext "JUNE 6 INVASION: NORMANDY" is then turned into the 21*21-pixel lattice QR code, as shown in Figure 3(a). With the help of a visual sharing scheme, the QR code can be converted into share '1' and share '2'. As shown in Figure 3(b) and Figure 3(c), each image is a 42*21 matrix. For each share, different probes are randomly selected from set α to produce the corresponding DNA chips. The probes in set α are fixed on the corresponding position of the glass or silicon chip, according to the positions of the black and white squares in the shared portion (the probes in subset α_0 are placed in the black square position, and the probes in subset α_1 are placed in the white square position), so that the plaintext is encrypted to two DNA chips. The encrypted chip can be sent to the receiver in a public way,

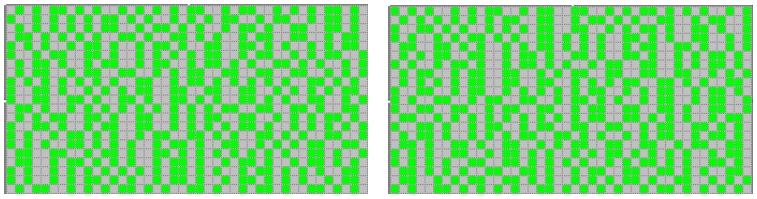
and the receiver can decipher the cipher text through the decryption key and the experimental condition. Due to the randomness of the probes, even for the same plaintext, the ciphertext chip won't be the same without the encryption process. In the actual cipher chip, the specific plaintext information cannot be obtained because there is no modified fluorescence on the probe.



(a) (b) (c)

Figure 3. Plaintext and ciphertext. (a) The QR code converted by plaintext, (b) ciphertext share '1', and (c) ciphertext share '2'

(3) **Extract information**. The receiving end obtains the ciphertext mixture, using the key and chip to carry out the hybridization reaction. After flushing the chip, the result is observed by CLSM and two decryption chip diagrams are obtained, as shown in Figure 4(a) and Figure 4(b). By recording and analyzing the information with a computer, the QR code of Figure 3(a) can be restored according to the principle of visual cryptography. It can be further converted to plaintext.



(a) (b)

Figure 4. Schematic diagram of the fluorescence labeling of the decrypted chip: (a) decrypted chip 1 and (b) decrypted chip 2.

4. Security analysis

The security of this encryption scheme is based on the security of algorithms and biotechnology. The first layer of security is biological safety, which is the main security of the system. The receiver can obtain the cipher text information by hybridizing the probe in the decryption key and the DNA chip. If the attacker wants to decipher the cipher text, he must know the decryption key. Because the decryption key is large in quantity, it is impossible for an attacker to guess. Therefore, it is difficult for an attacker to obtain plaintext on the DNA chip without a decryption key. In this scheme, to achieve higher security, we randomized the cipher text and made a DNA chip with different mixing of probes containing nucleotide sequences. Such DNA chip is more difficult to sequence. In addition, the combination of probes at each point can also change, so the hybridization results will also vary within a certain range. If the attacker simply finds some probes and a DNA chip to hybridize, because these probes are different from the decryption key probes, the hybrid signal obtained by the attacker and the hybrid signal obtained using the decryption key probes will be very different; there will be a huge error in the signal and it will be no help for decryption. Even if the attacker gets the probes in the decryption key, the correct cipher text information cannot be obtained without knowing the experimental conditions.

The second layer of security is the computational problem. If the first layer security has been broken down, it must have a strong computational capability to decipher the scheme. In this scheme, we hide the plaintext through DNA chip technology, and it is difficult for attackers to find the key words as a probe to decipher the cipher text. With the development of biotechnology, the probe on each point of the DNA chip can be identified efficiently, and the second layer of security also ensures high efficiency of the proposed scheme. The QR code in the scheme is in a 21×21 matrix form. The two shared copies are 21*42 pixels; each has two possibilities, information and no information. So, the cipher text has 2^{842} possibilities. The attacker wants to pick out the correct plaintext information from these possibilities, and it can be predicted that this task is similar to looking for a needle in a haystack. In addition, using the principle of visual encryption technology

to encrypt the plaintext, if we store the two shared copies of the keys separately, we will not get any information from the original plaintext, even if we get partial share information. Additionally, because the plaintext information is hidden in the fluorescent tag of the cDNA probe, the attacker cannot find the keyword as a probe to show the ciphertext. For the DNA chip of a probe n-order square matrix, each probe on the chip has two states: labeled fluorescence and unlabeled fluorescence. In the same way, its complementary chain also has two states. Therefore, each pixel of the chip has four states, and the probability of obtaining the correct combination of fluorescent tags is close to zero, even after acquiring the correct gene chip.

DNA chip technology is adopted in this paper, and the decryption phase does not need sequencing, unlike other reports in the literature [7]. Moreover [18], this method is more stable and easier to achieve. Compared with the literature [14], the security of this method is improved by combining secret sharing with the digital image by introducing a visual encryption algorithm.

5. Conclusions

Combined with DNA chip technology, a visual cryptography algorithm based on gene chip technology is constructed, which successfully integrates the advantages of the algorithm in information security with the natural advantages of modern biotechnology. An example is given to illustrate the implementation of the scheme. The security, practicality, and complexity of this algorithm are discussed in the fields of information security and biochemical technology. Through the above security analysis, we showed that the scheme has strong security. In addition, the two shared copies of the DNA chip can be implemented with a DNA chip. Share '1' and share '2' are placed on the upper and lower half of the chip, respectively. Thus, the cryptography is still secure without the decryption key. Similarly, the decryption key can also be put together. However, it is important that the probes do not produce non-specific hybridization. Although this has lost the meaning of sharing, the security of the system has not been reduced at all.

Of course, the encryption system proposed in this paper is not perfect. The cost of DNA chips is higher, the timeliness of the whole system is poor, and the encryption process and decryption process are time-consuming. With further improvement of biotechnology, it is believed that these two defects will be improved.

Acknowledgments

The work for this paper was supported by the National Natural Science Foundation of China (Grant Nos. 61602424, 61472371, 61572446, 61472372), Plan for Scientific Innovation Talent of Henan Province (Grant No.174100510009), Program for Science and Technology Innovation Talents in Universities of Henan Province (Grant No. 15HASTIT019) and Key Scientific Research Projects of Henan High Educational Institution (18A510020).

References

1. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," *Information and Computation*, vol. 129, no.2, pp. 86-106, 1996
2. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended Capabilities for Visual Cryptography," *Theoretical Computer Science*, vol. 250, no. 1-2, pp. 143–161, 2001
3. Y. C. Chen, "Fully Incrementing Visual Cryptography from a Succinct Non-monotonic Structure," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 5, pp. 1082-1091, 2017
4. L. Chiu and K.H. Lee, "User-friendly Threshold Visual Cryptography with Complementary Cover Images," *Signal Processing*, vol. 108, no. 3, pp. 476-488, 2015.
5. S. Cimato and C. N. Yang, "Visual Cryptography and Secret Image Sharing," CRC Press, Inc., Taylor &Francis, 2011
6. M. Gnanaguruparan and S. Kak, "Recursive Hiding of Secrets in Visual Cryptography," *Cryptologia*, vol. 26, no. 1, pp. 68-76, 2002
7. M. Hirabayashi, H. Kojima, and K. Oiwa, "Design of True Random One-Time Pads in DNA XOR Cryptosystem," *Natural Computing*, vol. 24, no. 3, pp. 174-183, 2010
8. Y. C. Hou, S. C. Wei, and C. Y. Lin, "Random-grid-based Visual Cryptography Schemes," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, no. 5, pp. 733-744, 2014
9. K. M. Kurian, C. J. Watson, and A. H. Wyllie, "DNA Chip Technology," *The Journal of Pathology*, vol.187, no. 3, pp. 267-271, 1999
10. Q. Liu, L Wang, A. G. Frutos, A. E. Condon, R. M. Corn, and L. M Smith, "DNA Computing on Surfaces," *Nature*, vol. 403, no. 6766, pp. 175-179, 2000
11. R. Lakshmanan and S. Arumugam. "Construction of a (k, n)-Visual Cryptography Scheme," *Designs Codes & Cryptography*, vol. 82, no. 3, pp. 629-645, 2017
12. G. C. Le Goff, L. J. Blum, and C. A. Marquette, "Shrinking Hydrogel-DNA Spots Generates 3D Microdots Arrays," *Macromolecular Bioscience*, vol.13, no. 2, pp. 227-233, 2013

13. T. Livache, B. Fouque, A. Roget, J. Marchand, G. Bidan, R. Téoule, and G. Mathis, "Polypyrrole DNA Chip on a Silicon Device: Example of Hepatitis C Virus Genotyping," *Analytical Biochemistry*, vol. 255, no. 2, pp. 188-194, 1998
14. M. X. Lu, X. J. Lai, G. Z. Xiao, and L. Qin, "A Symmetric Encryption Method based on DNA Technology," *Science in China (Series E)*, vol.37, no. 2, pp. 175-182.2007
15. M. Naor and A. Shamir, "Visual Cryptography," *Lecture Notes in Computer Science*, vol. 950, no. 9, pp. 1-12, Apr. 1995
16. M. Ogihara and A. Ray, "DNA Computing on a Chip," *Nature*, vol.403, no.6766, pp. 143-144, 2000
17. F. Praetorius, and H. Dietz, "Self-assembly of Genetically Encoded DNA-protein Hybrid Nanoscale Shapes," *Science*, vol. 355, no. 6331, eaam5488, 2017
18. S. Pramanik and S. K. Setua, "DNA Cryptography," *IEEE International Conference on Electrical & Computer Engineering*, vol. 90, no. 1, pp. 551-554, 2013
19. R. D. Prisco and A. D. Santis, "On the Relation of Random Grid and Deterministic Visual Cryptography," *IEEE Transactions on Information Forensics & Security*, vol.9, no. 4, pp. 653-665, 2017
20. E. Rasul, H. A. Abdul, and F.I. Ismail, "Chaos-based Image Encryption Using a Hybrid Genetic Algorithm and a DNA Sequence," *Optics and Lasers in Engineering*, vol. 56, no. 5, pp. 83-93, 2014
21. J. H. Reif and H. John, "Scaling Up DNA Computation," *Science*, vol.332, no. 6034, pp. 1156-1157, 2011
22. E. R. Verheul and H. C. A. Van Tilborg, "Constructions and Properties of *k* Out of n Visual Secret Sharing Schemes," *Design Codes and Cryptography*, vol. 11, no. 2, pp. 179-196, 1997
23. G. Wang, W. Yan, and M. Kankanhalli, "Content based Authentication of Visual Cryptography," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9427-9441, 2017.
24. X. Zhang, F. Han, and Y. Niu, "Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding," *Computational Intelligence and Neuroscience*, (online since August 20, 2017). (DOI 10.1155/2017/6919675)