Password Protected Visual Cryptography via Cellular Automaton Rule 30

Roman V. Yampolskiy[1], Jovan D. Rebolledo-Mendez[2], and Musa M. Hindi[3]

[1] Computer Engineering and Computer Science, University of Louisville, Louisville, USA
[2] BMB, University of Louisville, Louisville, USA
[3] Cerner Corporation, Kansas City, USA
{rvyamp01,jdrebo01}@louisville.edu,
musa.hindi@gmail.com

Abstract. Visual cryptography depends on two shares. The initial configuration, extra security bits and the number of the rule for the CA along with the number of computed steps serve as a password for a visually encrypted image. The second share could contain a predefined pattern; the developed algorithm uses a snapshot of a CA after a certain number of steps to generate the predefined share. Only one of these shares has to be random. The developed encryption system is a hybrid between visual and classical cryptographic approaches. It requires less storage space compared to a standalone visual encryption system and relies on Rule 30's tested statistically significant randomness.

Keywords: *C*ellular Automata, CA Rule 30, Cryptography, One Time Pad, Visual Cryptography.

1 Introduction

Visual cryptography [1-2] is broad in definition and applicability [3-23], and there are many methods used in encrypting visual data. In essence, an image is converted into one or more images, which in isolation convey no information whatsoever. However, with a proper means to decrypt those images, one can display the original data.

During Eurocrypt '94, Moni Naor and Adi Shamir [1] proposed a novel visual cryptographic method. Their method was based on the one time pad system of encryption. In its most basic form an image is split into two derived images or 'shares.' One share acts as a key and the other as a cipher. Each one, when viewed in isolation from the other, displays no meaningful data. However, when they are superimposed a discernible image can be viewed.

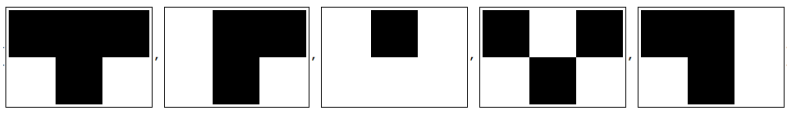
The advantage of their method lies in its security and practicality. It is completely secure due to the fact that without all the shares the original visual data cannot be retrieved. Also, the encrypted shares are generated in a random manner to ensure that no date can be retrieved from a single share. Its practicality on the other hand lies in computational decryption. Printing the shares on transparencies and superimposing them on top of one another will achieve the desired decryption.

Y.Q. Shi (Ed.): Transactions on DHMS IX, LNCS 8363, pp. 57–67, 2014.

Visual cryptography usually builds the first share in a completely random fashion. Then, using the original image's pixel data as well as the first share's random pixel data, the second complementary share is generated.

Despite the method's simplicity and practicality, the retrieval and decryption of the image requires presence of both shares. If one of the shares is missing, the decryption process becomes impossible. In addition, a single image of size n bytes has to be expanded, first by doubling each side and then by multiplying that by two.

If we can find a method that can deterministically generate a share based on a relatively small password, we can bypass the need for having two shares altogether. Our study proposes that Cellular Automata (CA) rules can be used to grow a share based on a predetermined start state. A cellular automaton can be very easily represented in a visual way as a bi-dimensional square grid, or composed by lines of cells. Each cell is either black or white, and in every subsequent step (or line), there is an applied rule that dictates which color that specific cell will be, based on the previous state color and its immediate neighbors. See Fig. 1 as an example of a cellular automaton.



(a) (b) (c) (d) (e)

Fig. 1. Grid showing an example of a cellular automaton rule. The rule makes a particular cell white if either of its neighbors are white (c) on the step before, and makes the cell black if both its neighbors were black (a, d) or black and white (b, e).

Differentiating from other works in security using CA [2, 24-31], our approach utilizes CA to address Visual Cryptography's issues, with the aid of Rule 30, by only requiring one share to be stored. By doing so it helps reduce the overall size of the encrypted image and preserve the ability to restore the original image with only one share.

Despite the abundance of computational capabilities, timing brute force attacks [32] could become an intensive computational task, increasing the time and processing exponentially, unlike context-free grammar passwords [33] and the use of password dictionaries [34-36]. Many times, the strength of written western alphanumeric passwords [37] is related to personal information such as common names and standard file names in Unix [38]. Additionally, employment of social engineering techniques can give attackers information about user passwords [39].

2 Approach

2.1 Original Visual Encryption Method

The original encryption method is derived from the one time pad visual encryption system proposed by Naor and Shamir at Eurocrypt '94. Its most basic form, a black and

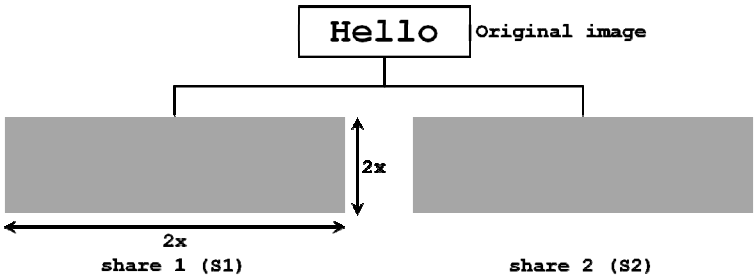


Fig. 2. This shows the generation of two encrypted shares from a single image

white image, is split into two shares (S1 and S2). Both S1 and S2 will have twice the length and width of the original image (see Fig.2).

Therefore, a single pixel in the original image is split into a set of four pixels. Any set of four pixels derived from the original pixel will alternate in color: black-white-white-black or white-black-black-white (see Fig. 3-a).

The specific order of the pixels in each four-pixel set in S1 is generated randomly. The order in the complementary share, 'S2', however, is not random. S2 is generated based on the original pixel in the original image as well as the color and order of pixels in S1 (see Fig. 3-b).

If the original pixel is black, the two complementary pixels, when superimposed, should produce four subsequent black pixels (see Fig. 3-c). If, on the other hand, the original pixel is white, the superimposed pixels should still alternate producing a pseudo-grey color resulting from the alternating black and white pixels.

As a result, it is clear that this method is completely secure since the share is initially randomly generated. There is no way to tell whether a set of four pixels in an encrypted share is derived from a black or white pixel by just looking at one share. Fig. 3 summarizes the visual encoding process.

2.2 Cellular Automata

A Cellular Automaton is a discrete model that represents a number of parallel entities that interact with one another in a way that influences their evolution and development. Simply put, a binary Cellular Automaton can be represented by an n-dimensional array where each member (i.e. cell) is an entity. Each entity normally has one of two states, 1 or 0. The state that a cell assumes in a given iteration is dependent on a set of rules that govern how a cell evolves from one iteration to the next in accordance with the cell's state and its neighbors' states.

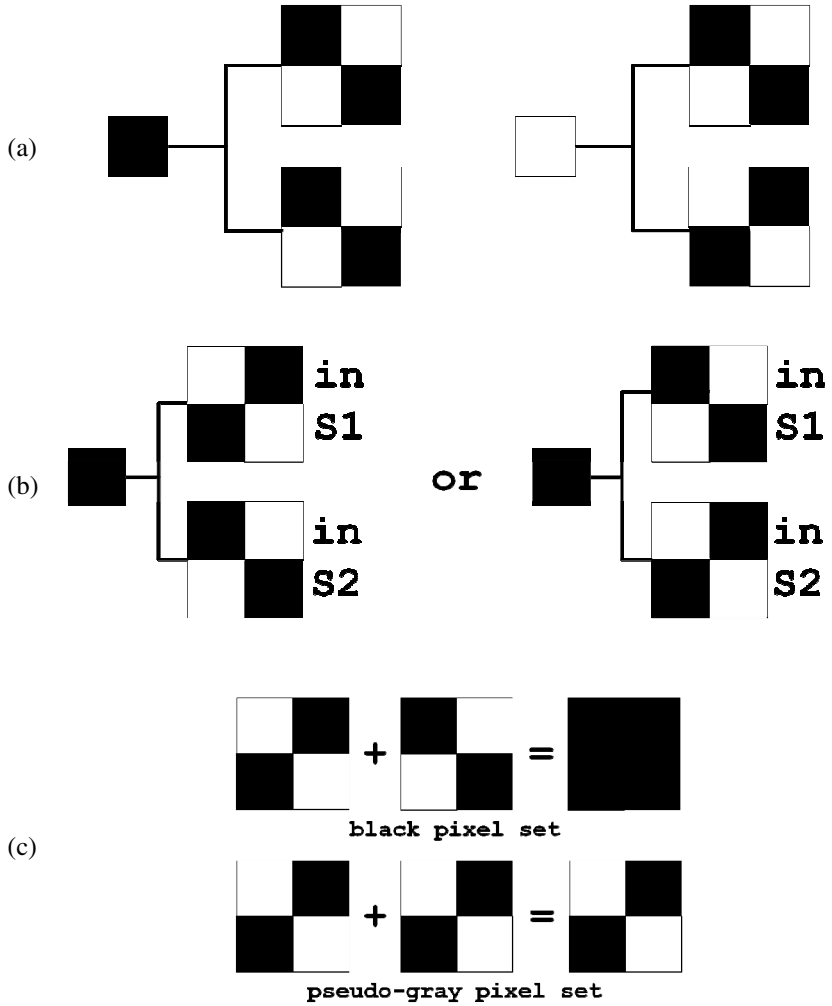


Fig. 3. (a) Possible sets of 4 pixels generated in share 1 and share 2 from encrypting a white or black pixel. (b) Two possible sets of 4 pixels generated in share 1 and share 2 from encrypting a black pixel. (c) The result of superimposing corresponding sets of 4 pixels.

This field of computational sciences dates back to the mid 1900s where it was the interests of the likes of Stanislaw Ulam, John von Neumann and John Conway. It is very impressive in its capacity to generate complex patterns from a simple set of rules and conditions. This capacity is utilized here to grow a seemingly random share by specifying a password as the initial condition and using a CA rule to grow the share. The specific rule chosen to carry out this task is rule 30.

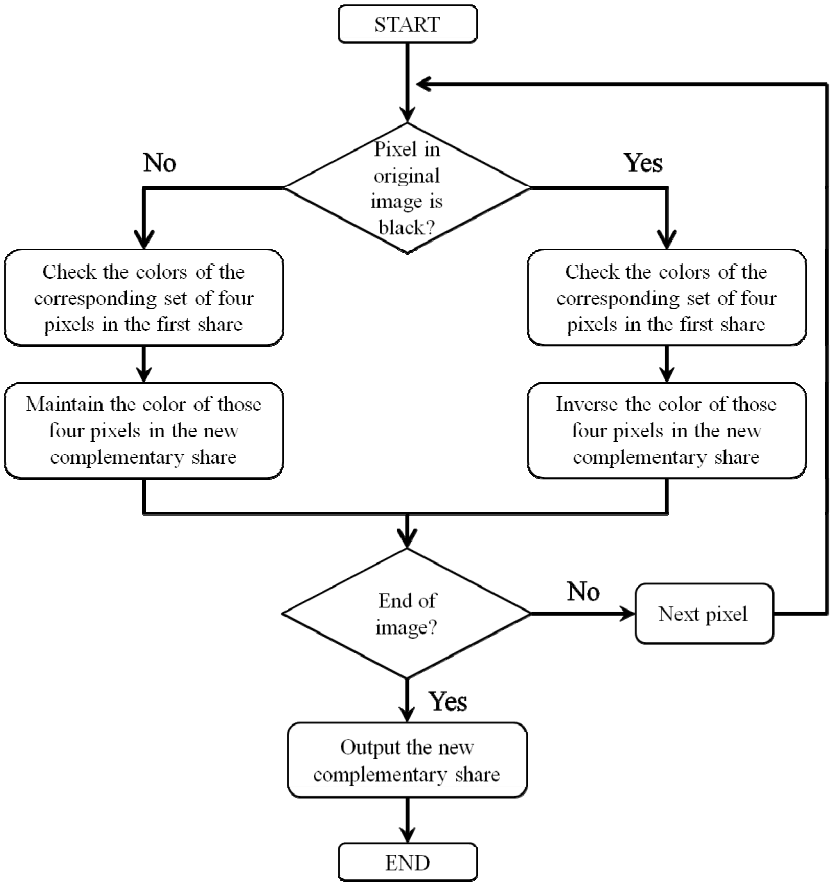


Fig. 4. Summary of the proposed visual encoding process

2.3 Rule 30

Rule 30 is one of the one-dimensional binary CA rules introduced by Stephen Wolfram in 1983 [40]. A cell's subsequent color is specified by the color of its immediate neighbors. The rule is named "Rule 30" (see Fig. 5) because the rule outcomes are encoded in the binary representation of $30 = 00011110_2$.

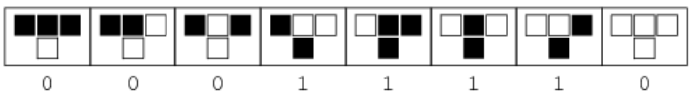


Fig. 5. Rule 30. This rule is used to grow a share that acts as the key to both encryption and decryption of an image.

2.4 Visual Encryption via Cellular Automata

In the original visual cryptography methodology, the first share is produced randomly, without any predefined rule or pattern. Following the typical visual cryptography method, the second and complementary share is generated based on the original image's pixel information and the pixel pattern in the first share. As a result, every visual encryption needs to have both shares in order to generate the original image. Contrasting with the common visual cryptography, our proposed method uses the CA rule 30 and only one share from the original image, instead of the common method in visual encryption where two shares are needed.

One of the many capabilities of a CA is that of generation or growth of patterns based on a simple set of initial rules. Dr. Stephen Wolfram provides evidence that randomness is found in the sequence generation in the time sequences that are created from running certain CA rules [41]. This capacity of random production can be exploited in visual cryptography so we could generate a complete share, starting with no more than a relatively small password taken from an image.

To encode an image using this method, a password would need to be generated. As an example for proving this method, the password is predefined to be 100 bits as a minimum size. The value of the password is extracted from the first row of pixels in the original image. If the first row is not sufficient to generate a 100-bit password, random bits are padded on to complete the 100 bits (but as a practical matter, this is not restricted to that number of bits, and could be greater than that). The CA rule 30 initial conditions are (i) the randomized first row and (ii) the initial two-color pixelized picture (see Fig. 6), with the picture's initial width and height.

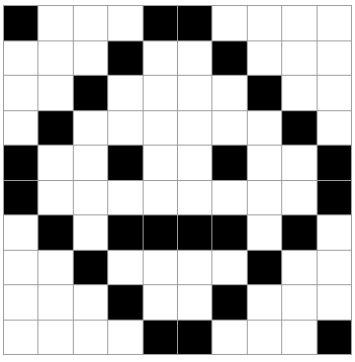


Fig. 6. Original Image: Picture= {{1,0,0,0,1,1,0,0,0,0}, {0,0,0,1,0,0,1,0,0,0}, {0,0,1,0,0,0,0,1,0,0},{0,1,0,0,0,0,0,0,1,0},{1,0,0,1,0,0,1,0,0,1},{1,0,0,0,0,0,0,0,0,1},{0,1,0,1,1,1,1,0,1,0},{0,0,1,0,0,0,0,1,0,0},{0,0,0,1,0,0,1,0,0,0},{0,0,0,0,1,1,0,0,0,1}}

ECA rule 30, with a window size of 200, appears to be adequate as a random number generator [42], passing all but one statistical test out of complete set of NIST statistical tests for randomness [43].

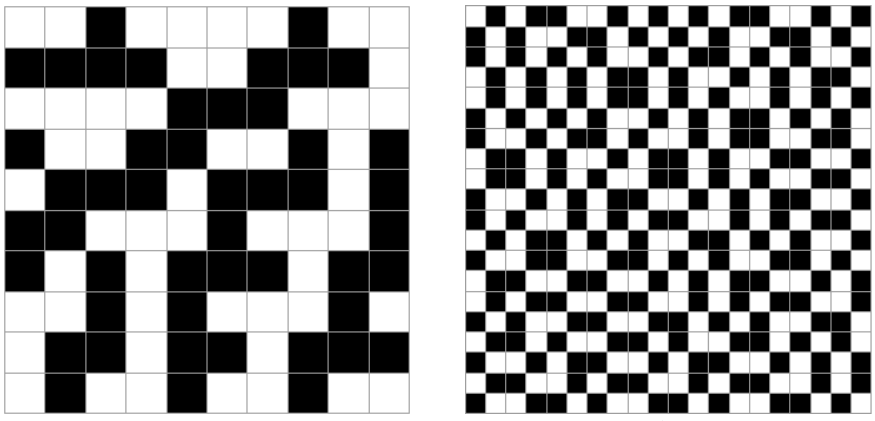
In the implementation of this methodology, the encryption and decryption process were programmed in Wolfram Mathematica. The following pseudocode is based on the Mathematica code that demonstrates how that was achieved starting with the original image as shown below.

```
If size appropriate
  Create matrix of password for CA
  Create cellular automaton rule 30
  Replace all values "1" for found in matrix password
  Create initial conditions for cellular automaton and
    extra bits
  Generates cumulative sums of the elements in the list
  Concatenates the two lists
  Creates matrix of trimmed lists
  Create cellular automaton rule 30, initial conditions
    of concatenation of the two lists
```

Each pixel in the CA grown share is then represented by 4 pixels:

```
While reading the matrix of the original image
  Make Share1 by replacing elements, assigning 1 to the double
size of the original image
  Create new image
```

Afterwards, the second share can be generated using the original image's pixel data and the relative organization of pixels in the CA grown share, which is similar to the original Visual Cryptography method, being able to utilize one single share (Fig. 7).

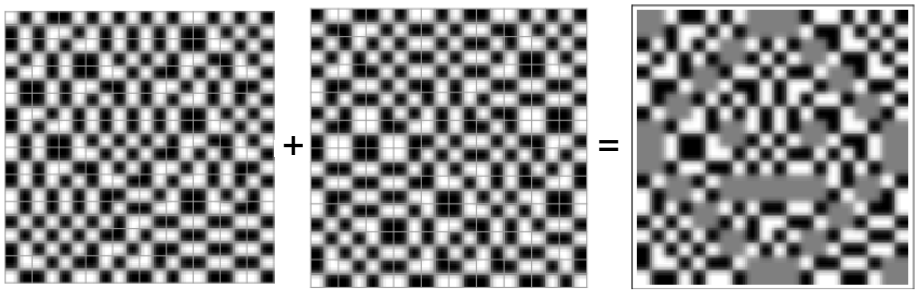


(a) (b)

Fig. 7. (a) Generation of a random share from the CA rule 30 and initial conditions. The minimum password size = 100 bits regardless of original image size. (b) The random share with each pixel represented by 4 alternating black and white pixels.

2.5 Visual Decryption via Cellular Automata

The output of the encryption process is a single share (Fig. 8). The password used for the encryption process is needed to decrypt the share and retrieve the original image. That password along with rule 30 is used to generate the other share needed to produce the original image. Similar to the initial stage in the encryption process, the password is used to grow the share. That share's pixels are then represented by four pixels each. Finally, the original image can be retrieved by superimposing the CA grown share with the single encrypted share. In a post-processing method, the image can be cleaned up by just changing the color of the gray into white.



(a) (b) (c)

Fig. 8. Visual Decoding Process: the addition of the shares (a) and (b) reconstruction of the original image (c)

Discussion

The original Visual Cryptography method usually relies on a one-time pad encryption method. Two shares are generated, where one acts as a cipher while the other acts as a key. Both the cipher and its respective key have to be present in image formats. Moreover, each of those images is double the width and double the height of the original image's dimensions. The resultant size increase per image ends up at eight times the original image's size. This is a large size increase in addition to the inconvenience of storing two separate shares per image.

Our method solves these two issues. We only need to store a single encrypted share and that share acts as our cipher. To decrypt the share, a visual key needs to be present. Unlike the original method, however, the key does not have to be stored as a full share. We only need the original 100-bit password, and from it an entire visual key can be grown via CA Rule 30.

This method is not more convenient as a result of storing a single share rather than two, but also more efficient. Only a single share needs to be stored, which is four times the size of the original image and half the size required by the common method.

Conclusion

The method described here builds on the original Visual Cryptography method presented by Naor and Shamir. It utilizes CA's ability to generate pseudorandom patterns from a simple starting point to grow a share from a predefined password. This approach is both more convenient and efficient than the original Visual Cryptography approach. A working demonstration of this research can be found in the Wolfram Demonstration Project site [44].

Acknowledgements. The authors of this manuscript would like to thank Dr. Stephen Wolfram for his guidance and support in crafting this methodology, as well as his great feedback. Also, we want to thank our NKS SS 2011 teachers, coaches and fellow students of that summer: it was a great learning experience.

References

1. Naor, M., Shamir, A.: Visual Cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Rong-Jian, C., Yuan-Hsin, C., Chao-Shen, C., Jui-Lin, L.: Image Encryption/Decryption System using 2-D Cellular Automata. In: Proceedings of the IEEE Tenth International Symposium on Consumer Electronics (ISCE 2006), St. Petersburg, Russia, pp. 1–6 (2006)
3. Abboud, G., Marean, J., Yampolskiy, R.V.: Steganography and Visual Cryptography in Computer Forensics. In: Proceedings of the Fifth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2010), Oakland, USA, pp. 25–32 (2010)
4. Losavio, M., Hindi, M., Yampolskiy, R., Wilson Keeling, D.: Boundary Conditions for the Digital Forensic Use of Electronic Evidence and the Need for Forensic Counter-Analysis. In: Proceedings of the Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2010), in Conjunction with IEEE Security and Privacy Symposium, Oakland, USA, pp. 1–6 (2010)
5. Arazi, B., Dinstein, I.H., Kafri, O.: Intuition, perception, and secure communication. IEEE Transactions on Systems, Man and Cybernetics 19(5), 1016–1020 (1989)
6. Spanos, G.A., Maples, T.B.: Security for real-time MPEG compressed video in distributed multimedia applications. In: Proceedings of the IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications, Scottsdale, USA, pp. 72–78 (1996)
7. O'Gorman, L., Rabinovich, I.: Photo-image authentication by pattern recognition and cryptography. In: Proceedings of the 13th International Conference on Pattern Recognition, Vienna, Austria, vol. 3, pp. 949–953 (1996)
8. Piva, A., Barni, M., Bartolini, F., Cappellini, V.: DCT-based watermark recovering without resorting to the uncorrupted original image. In: Proceedings of the International Conference on Image Processing, Santa Barbara, USA, vol. 1, pp. 520–523 (1997)
9. Main, P.M.: Extension of secure audio and video data from the NTC through the public switched telephone network. In: MILCOM 1997, Monterrey, USA, vol. 1, pp. 228–231 (1997)

10. O'Ruanaidh, J.J.K., Pun, T.: Rotation, scale and translation invariant digital image watermarking. In: Proceedings of the International Conference on Image Processing, Santa Barbara, USA, vol. 1, pp. 536–539 (1997)
11. Dugad, R., Ratakonda, K., Ahuja, N.: A new wavelet-based scheme for watermarking images. In: Proceedings of the International Conference on Image Processing 1998 (ICIP 1998), Chicago, USA, vol. 2, pp. 419–423 (1998)
12. O'Gorman, L., Rabinovich, I.: Secure identification documents via pattern recognition and public-key cryptography. IEEE Transactions on Pattern Analysis and Machine Intelligence 20(10), 1097–1102 (1998)
13. Sang-Yi, Y., Kyo-II, C., Chung-Sang, R., Kwang-Hoon, C.: Encryption of cell-oriented computer generated hologram by using visual cryptography. In: The Pacific Rim Conference on Lasers and Electro-Optics (CLEO/Pacific Rim 1999), Seoul, South Korea, vol. 3, pp. 817–818 (1999)
14. Stinson, D.: Visual cryptography and threshold schemes. IEEE Potentials 18(1), 13–16 (1999)
15. Fridrich, J.: Applications of data hiding in digital images. In: Proceedings of the Fifth International Symposium on Signal Processing and its Applications (ISSPA 1999), Brisbane, Australia (1999)
16. Ran-Zan, W., Chi-Fang, L., Ja-Chen, L.: Hiding data in images by optimal moderately-significant-bit replacement. Electronics Letters 36(25), 2069–2070 (2000)
17. Anbarasi, L.J., Vincent, M.J., Mala, G.S.A.: A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography. In: Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, pp. 129–133 (2011)
18. Zhi, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography. IEEE Transactions on Image Processing 15(8), 2441–2453 (2006)
19. Liu, F., Wu, C.K., Lin, X.J.: Colour visual cryptography schemes. IET Information Security 2(4), 151–165 (2008)
20. Jaya, M.S., Aggarwal, A., Sardana, A.: Novel authentication system using visual cryptography. In: Proceedings of the World Congress on Information and Communication Technologies (WICT), Mumbai, India, pp. 1181–1186 (2011)
21. Chavan, P.V., Atique, M.: Design of hierarchical visual cryptography. In: Proceedings of the 2012 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, pp. 1–3 (2012)
22. Monoth, T., Babu, A.P.: Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns. In: Proceedings of the International Conference on Cyberworlds (CW), Singapore, pp. 171–178 (2010)
23. Prema, G., Natarajan, S.: Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application. In: Proceedings of the International Conference on Information Communication and Embedded Systems 2013 (ICICES), Chennai, India, pp. 727–730 (2013)
24. Ismail, I.A., Abdo, A.A., Amin, M., Diab, H.: Self-Adaptive Image Encryption Based on Memory Cellular Automata. Proceedings of the International Journal of Information Acquisition 8(3), 227–241 (2011)
25. Kari, J.: Cryptosystems based on reversible cellular automata (1992)
26. Machhout, M., Guitouni, Z., Zeghid, M., Tourki, R.: Design of Reconfigurable Image Encryption Processor Using 2-D Cellular Automata Generator. International Journal of Computer Science & Applications 6(1), 43–62 (2009)

27. Seredynski, F., Bouvry, P.P., Zomaya, A.Y.: Cellular automata computations and secret key cryptography. Parallel Computing 30(5-6), 753–766 (2004)
28. Hernández Encinas, L., Martín del Rey, Á., Hernández Encinas, A.: Encryption of Images with 2-dimensional Celluar Automata. In: Proceedings of the 6th World Multiconference on Systemics, Cybernetics and Informatics and 8th International Conference on Information System Analysis and Synthesis (SCI/ISAS 2002). International Institute of Informatics and Systemics (IIIS), Orlando (2002)
29. Álvarez Marañón, G., Hernández Encinas, L., Martín del Rey, Á.: A new secret sharing scheme for images based on additive 2-dimensional cellular automata. In: Marques, J.S., Pérez de la Blanca, N., Pina, P. (eds.) IbPRIA 2005. LNCS, vol. 3522, pp. 411–418. Springer, Heidelberg (2005)
30. Guan, P.: Cellular Automaton Public-Key Cryptosystem. Complex Systems 1, 51–57 (1987)
31. Wolfram, S.: Cryptography with Cellular Automata. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 429–432. Springer, Heidelberg (1986)
32. Trostle, J.T.: Timing attacks against trusted path. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, USA, pp. 125–134 (1998)
33. Weir, M., Aggarwal, S., deMedeiros, B., Glodek, B.: Password Cracking Using Probabilistic Context-Free Grammars. In: Proceedings of the 30th IEEE Symposium on Security and Privacy, Berkeley, USA, pp. 391–405 (2009)
34. Narayanan, A., Shmatikov, V.: Fast dictionary attacks on passwords using time-space tradeoff. In: Proceedings of the 12th ACM Conference on Computer and Communications Security, Alexandria, USA, pp. 364–372 (2005)
35. Klein, D.V.: Foiling the cracker: A survey of and improvements to password security. In: Proceedings of the USENIX UNIX Security Workshopp, Portland, USA (1990)
36. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: empirical results. IEEE Security & Privacy 2(5), 25–31 (2004)
37. Kessler, G.C.: Passwords - Strengths and weaknesses. Gary Kessler Associates (1996), http://www.garykessler.net/library/password.html (January 4, 2013)
38. Yampolskiy, R.V.: Analyzing User Password Selection Behavior for Reduction of Password Space. In: Proceedings of the 40th Annual IEEE International Carnahan Conferences Security Technology, Lexington, USA, pp. 109–115 (2006)
39. Mann, I.: Hacking the human (IT - Security). Engineering & Technology 3(1), 62–63 (2008)
40. Wolfram, S.: A New Kind of Science. Wolfram Media, Inc., Champaign (2002)
41. Wolfram, S.: Random sequence generation by cellular automata. Advances in Applied Mathematics 7(2), 123–169 (1986)
42. Gage, D., Laub, E., McGarry, B.: Cellular Automata: Is Rule 30 Random? In: Proceedings of the Midwest NKS Conference, Indiana University (2005)
43. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A.I., Dray, J., Vo, S.: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptologic Applications. NIST Special Publication 800–822. NIST (2001)
44. Yampolskiy, R.V.: Single-Share Password-Protected Visual Cryptography via Cellular Automata (2011), http://demonstrations.wolfram.com/SingleSharePasswordProtectedVisualCryptographyViaCellularAut/ (cited January 15, 2013)