

OCA: An intelligent model for improving security breach of biometric based authentication systems

Sandeep Kumar Sharma *

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Anil Kumar [†]

Department of Computer Science and Engineering

Poornima Institute of Engineering and Technology, Jaipur

Jaipur

Rajasthan

India

Rashmi Ashtagi [§]

Department of Computer Engineering

Vishwakarma Institute of Technology

Bibwewadi

Pune 411037

Maharashtra

India

Rekha Jain [‡]

Department of Computer Application

Manipal University Jaipur

Jaipur

Rajasthan

India

* E-mail: sandeep.sharma@jaipur.manipal.edu (Corresponding Author)

[†] E-mail: anil.vashu@gmail.com

[§] E-mail: rashmiashtagi@gmail.com

[‡] E-mail: rekha.jain@jaipur.manipal.edu

Abstract

In the recent era, biometrics is one of the most used authentication systems. Generally, biometric systems are based on imaging technology, which works on scanned images. This system processes the image and compares it with the database and decides authenticity of user. Authentication and faster response are the key objectives of all biometric systems, but they suffered from a serious issue i.e., security breach. In this article, a Cellular Automata based method is introduced, which processes the image and identify possible security breaches. The proposed method analysis all the pixels of the image and maps a rule, which processes the image and generates a gray image by defining all the possible edges of the image objects. The gray image contains only binary values, which may reduce the chance of breach and decrease the comparison time of gray image with database. In this paper, the proposed method is experimented on the open-source dataset and the results are validated using authentication parameters.

Subject Classification: Primary 03B70, Secondary 03D10.

Keywords: Biometric, Authentication, Cellular automata, Edge, Transition function.

1. Introduction

Biometric is an extremely frequent technique, used in the authentication systems from last decade. This technique makes the authentication system faster and more secure as compared to password-based authentication systems. Generally, password-based systems have some limitations i.e., cracking, password remembering, surfing attacks etc., but biometric systems overcome these limitations [5]. Despite these pluses, biometric systems are suffering from the following issues.

- Hackers may steal the data of authentication system. Once the data of biometric system is breached, recovery of data is very difficult.
- Erroneous recognition and wrong rejection of the users.

Generally, the biometric systems have the following key process:

- A. Enrollment: The admin of the system enrolls the features of users to the biometric authentication system.
- B. Verification: During login to the biometric system, an image is scanned by sensor and process the image to extract features of image.
- C. Identification: In this process, the matcher compares the extracted features with database and define identity of the user. The matcher notifies the user about authentication and rejection.

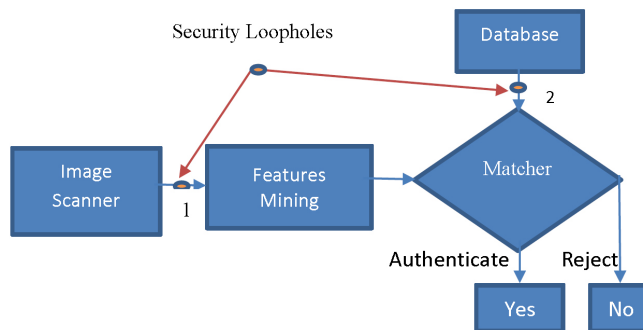


Figure 1
Biometric Authentication System Process

Figure 1 shows the process of a biometric system and places where security loopholes are probable. The red circled spots represent a place where security breaches are possible. At the time of scanning image, attackers may attack the system and provide a false input to the system. This practice may deny the authentic users to avail the services. During the input image features mining process, if the features are not properly mined, and attacked then the user will not be authenticated. The authentication system needs to mine exact features and should prevent the attackers for further updating the mined features. The proposed research is introducing a Cellular Automata based method, which analysis the scanned image and processes the image to find exact image features.

Cellular automata technology (CAT) has the capability to process different types of images i.e., colored, noisy, shaded, reflected, and night vision images. Generally, the images are formed using several pixels and these pixels are arranged in the form of cells or grids. The CAT works on image pixels by defining a rule or transition function. The rule is defined by analyzing outer pixels of all the pixels of image. This may help the system to detect existing breaches in the image. The transition function of the CA processes the pixels or current state of scanned image generates a new pixel or state. The flow chart shown in figure 2 represents the working of CAT on scanned image $S_{M,N}$, where M and N are the size of image [6].

The remaining contents of the article are organized as follows. In section 2, we discussed literature survey of the existing research. Section 3 of the article discusses proposed methodology with numerical analysis. Section 4 demonstrates experimental and comparative study of the research. Finally, in section 5 we conclude the proposed work and future scope of the work.

2. Literature Survey

Biometrics is not new research; it came in the market from 14th century. At the beginning, this technology was used for fingerprint detection. Later a lot of relevant applications have been introduced in the market, but since the 1960's this technology was in used for authentication purpose.

As the users of biometrics authentication system increases, security issues are also arising. So, there are still some rooms available in this technology, where improvement is required. Due to popularity and security issues of biometrics authentication system, the authors were motivated to overcome the issues. Mostly, biometric systems work on imaging technologies. This section of the research represents a survey on biometric authentication systems and imaging technologies.

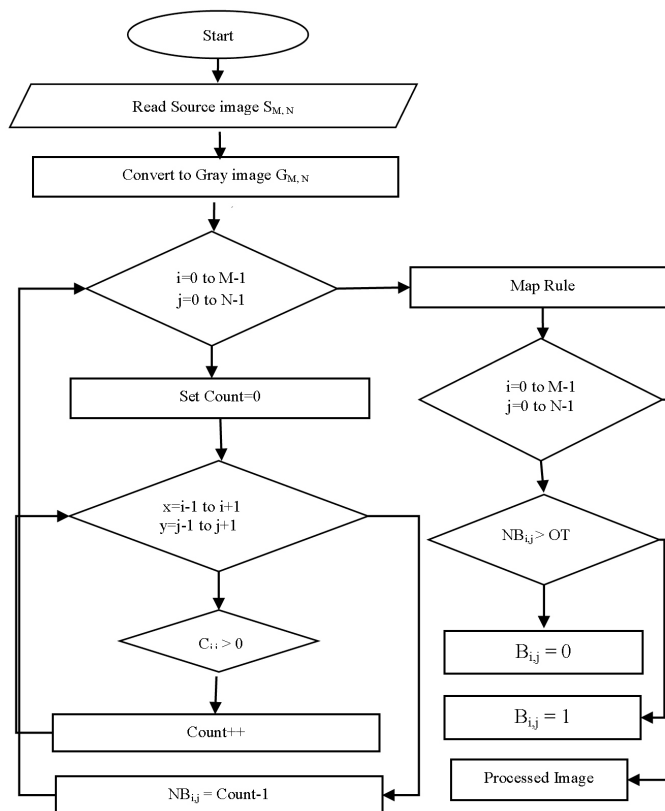


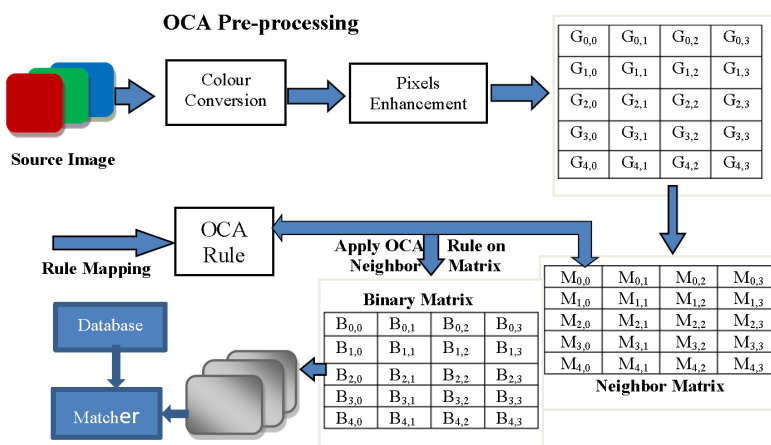
Figure 2

Working Mechanism of Cellular Automata Technology

Gaurav Meena et al. [2019] introduced a biometric based authentic to secure network system. In this IoT and machine learning concepts was used to implement proposed method [1]. **Anil Kumar et al. [2022]** introduce a cellular automata-based method for securing information. In this research a cryptographic method was implemented using processing digital images [2]. **Har Om et al. [2017]** discussed a session key based biometric authentic system. A message Digest algorithm was used to protect scanned image of user [3]. **Sapna Sharma et al. [2021]** generated a vascular pattern to improve security of biometric authentic system [4]. **Baby Sherin et al. [2017]** presented a paper based on particle swarm optimization method for image edge detection. This method implemented a global fitness method by analyzing homogeneous pixels then comparing them with all the pixels to detect final edges. The proposed method challenged for 70% accuracy with minimum time [12]. **Jianfang Cao et al. [2018]** presented a paper for parallel image edge detection algorithm using improved Otsu-Canny method for Hadoop platform. The proposed method smoothed source images using Gaussian operator by dividing gradients into clockwise and anti-clockwise 8 directions. The proposed method decreases running time up to 67.2 % [7]. **Zeyang Dou et al. [2017]** presented a paper for image smoothing based on Truncated Total Variation method. In this paper a common threshold is introduced for smoothing pixels which suffer from gradient penalties. The proposed method smoothed the images by removing noises, texture, and artifacts restoration. The produced image smoothed by total variant method is comparatively small and SNR value is large [8]. **Dongping Wang, et al. [2020]** developing a model for enhancing image visualization features by adjusting sharpness of image. In this model, a common threshold is calculated using the first and second order derivation of set of pixels. The proposed model is experimented on different color components of color image and claims approximate 99% accuracy [9]. **Zhong-xun Wang et al. [2018]** proposed a method with aimed of decrease traffic accidents by implementing a real time automatic application which can detect road lane lines and boundary edges. The proposed method performs convolution operations in 8 different directions to obtain robust road image edges [10].

3. OCA Model

The Cellular Automata Technology (CAT) can explore data which is either in one-dimensional (1D) or two-dimensional (2D). The source data of the proposed research is of two-dimensional types, so the two-dimensional



approach outer cellular automata (OCA) is used to process the image to find existing edges [13]. The OCA method analysis all the pixels of gray scale image and embedded all the pixels which have similar intensity pixels. The OCA method applies their functions on the embedded pixels and finds desired results. Figure 3 represents fundamental configuration design of the proposed methodology using OCA technology. In this proposed methodology six steps are implemented i.e., Pre-processing, Neighbor matrix generation, Map OCA rule, edge detection course, post-processing and matcher.

3.1 OCA Pre-processing

The working of proposed OCA method starts with reading of color space image (RGB, HSV and YUV), Gray scale image, Black and white image. The source image may be noisy or noise free image. The noisy image may be a blurred and breached image and the noise free image is original image. This step of the proposed research enhanced the quality of scanned image by deblurring the pixels and produced gray scale image and each pixel of the produced image is represented using 8 bits. Equations 1,2, and 3 are used to enhance the quality of scanned image. Consider S_{IMG} is the scanned image and E_{IMG} is the enhanced image.

$$G_{IMG} = \sum \begin{matrix} S_{IMG}(255,0,0) * 30 / 100, \\ S_{IMG}(0,255,0) * 59 / 100, \\ S_{IMG}(0,0,255) * 11 / 100 \end{matrix} \quad (1)$$

$$AR_{M,N} = \begin{bmatrix} G_{-1,-1} & \cdots & G_{-1,N} \\ \vdots & G_{IMG} & \vdots \\ G_{M,-1} & \cdots & G_{M,N} \end{bmatrix} * \frac{1}{9} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad (2)$$

$$E_{IMG} = E_{i,j} = \bigcup_{\substack{i=M-1 \\ j=N-1 \\ i=0 \\ j=0}} G_{i,j} \text{ if } G_{i,j} < AR_{i,j} \text{ then } G_{i,j} = A_{i,j} \quad (3)$$

3.2 Neighbor Matrix Generation

The neighbor matrix shows the number of live members for all the pixels of enhanced source image. The neighbor matrix considers surrounding 8 neighbors i.e., left, right, up, down, and diagonal. Hence the matrix contains values from 0 to 8. The following nbrCount () algorithm is used to create the neighbor matrix.

Algorithm 3.1: nbrCount() algorithm

Step 1: Read Enhanced Image $SI_{M,N}$
 Step 2: for $i=0$ to $M-1$ and $j=0$ to $N-1$
 Set count=0
 Set $P=0$ if $i=0$ otherwise $P=i-1$
 Set $Q=0$ if $j=0$ otherwise $Q=j-1$
 Set $R=M$ if $i<M-1$ otherwise $R=M-1$
 Set $S=N$ if $j<N-1$ otherwise $R=N-1$
 for $x=P$ to R and $y=Q$ to S
 if $SI[x][y]>0$
 Count++
 NBR[i][j]=count-1

3.3 Map OCA Rule

The OCA rule is decided according to the values of cells in neighbor matrix. The neighbor matrix has 9 possible values, the smallest value is 0 and the largest value is 8, such that from 0 to 8. The CA has a number of rules according to neighborhood. The proposed method decides the

efficient rule for edge detection according to loneliness and overpopulation of the cell. So, an effective rule needs to be mapped for processing the images and producing efficient results. This section of the research analyzes enhanced source image NBR_{img} and defines a transition function. The transition function of OCA is estimated according to equations 4, 5, and 6. The T_1 and T_2 work as a transition function of the proposed method for the source image.

$$m = \text{Min}(NBR_{M,N}) \quad (4)$$

$$n = \text{Max}(NBR_{M,N}) \quad (5)$$

$$T_1 = \frac{\sum_{i=m}^{i=n} i}{n+1} \quad (6)$$

$$T_2 = \frac{\sum_{i=m}^{i=n} i - \sum_{i=m}^{i=T_1-1} i}{n - T_1 + 1} \quad (7)$$

and threshold function considers only those cells whose number of neighbors is between 4 and 6. The threshold function makes all the considered cells to live cells and remaining cells to dead cells. The value of live cells is set to 1 and dead cells value is set to 0.

3.4 Edge Detection Course

Once the OTCA rule or transition function is decided, it should be applied on all the cells of the neighbored matrix. The threshold function works as a global or unique function which read the current state of the cell and generates new state. The transition function decides the new state of the cells according to equations 8 and 9.

$$\text{New}_{i,j} = \text{Alive if } NBR_{i,j} \geq T_1 \text{ and } NBR_{i,j} \leq T_2 \quad (8)$$

$$\text{New}_{i,j} = \text{Dead if } NBR_{i,j} < T_1 \text{ or } NBR_{i,j} > T_2 \quad (9)$$

The OCA rule finds the cells which are alive, and the current state is happiness, loneliness, or over-population. The proposed method changes their current state to new state according to current state and transition function. The output New_{img} of this step, may suffer from different types of noise. So, the first step of the proposed research should be applied again to smooth the blurred pixels.

3.5 Post Processing

The produced output after applying all the steps is in the form of binary matrix, but the result should be in the form of image. So, the last step post processing of the proposed OCA method is used to transform the binary matrix into the color image by converting value 1 to black and value 0 to white pixel. The determined edges of the source image are shown by black colors or gray scale.

3.6 Matcher

The edges produced by OCA method are accurate, continuous, and protected. The matcher compares these edges with database and respond in quick manner, because the matcher compares only specific features of image.

4 Result Discussion

In this article, the proposed method is experimented on SOCOFing dataset of Kaggle. The accuracy of the results is measured by analyzing authentication parameters i.e., false accepting and rejection rates. Approximate 1000+ data are used to validate the desired accuracy of the research. Table 1 depicts a confusion matrix on dataset “100_M_Left_Index_finger” and table 2 depicts accuracy of only 5 selected data.

The accuracy of the proposed method is measured using equation 10, where FP, FN, TP, TN represent false positive, false negative, true positive, and true negative [11].

$$Accuracy = \frac{FP+TP}{FP+FN+TP+TN} \quad (10)$$

Table 1
Confusion matrix

	Actual Image Features	
Extracted Image Features	1879	56
	176	19

Table 2
Accuracy measurement of the proposed OCA method

Class Label	Accuracy
100_M_Left_Index_finger	96.47 %
101_M_Left_Index_finger	98.12 %
100_M_Right_Index_finger	95.33 %
102_M_Left_Little_finger	94.25 %
103_M_Left_index_finger	96.50 %

5. Discussion and Conclusion

This research proposed an OCA model for improving security of biometric authentication system. The OCA model is able to provide security to the biometric based authentication at scanning of user's image. The model extract image features by analyzing outer neighbor pixels and maps a rule using extracted features. This rule applied on the scanned image and produced a unique protected image. The matcher of the proposed research compares the produced with database and decide authenticity of the user. The result discussion section of the article expresses that, the acceptance rate of authentic user is approximate 96%.

The proposed method is unable to prevent the attackers to enter in system at the time of matcher's activities. Database security is also an issue with these system; to follow network security measures, we can resolve the issues

Abbreviations

OCA	Outer Cellular Automata
CAT	Cellular Automata Technology
SOCOFing	Sokoto Coventry Fingerprint

References

- [1] Gaurav Meena & Sarika Choudhary. Biometric authentication in internet of things: A conceptual view, *Journal of Statistics and Management Systems*, 22:4, 643-652 (2019).
- [2] Kumar, A., & Sharma, S. K. Information cryptography using cellular automata and digital image processing. *Journal of Discrete Mathematical*

- Sciences and Cryptography*, 25(4), 1105-1111 (2022). <https://doi.org/doi.org/10.1080/09720529.2022.2072437>.
- [3] Hari Om & Subhasish Banerjee. A password authentication method for remote users based on smart card and biometrics, *Journal of Discrete Mathematical Sciences and Cryptography*, 20:3, 595-610 (2017).
 - [4] Sapna Sharma & Shilpy Agrawal. Personal authentication based on vascular pattern using finger vein biometric, *Journal of Discrete Mathematical Sciences and Cryptography*, 24:5, 1167-1178 (2021).
 - [5] H. D. Supreetha Gowda, G. Hemantha Kumar & Mohammad Imran. Multi-modal biometric system on various levels of fusion using LPQ features, *Journal of Information and Optimization Sciences*, 39:1, 169-181 (2018).
 - [6] S. K. Sharma, C. S. Lamba, and V. S. Rathore, "Radius based cellular automata approach for image processing applications," *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-5 (2017), doi: 10.1109/ICCCNT.2017.8203990.
 - [7] J Cao, L Chen, M Wang and Y Tian, "Implementing a Parallel Image Edge Detection Algorithm Based on the Otsu-Canny Operator on the Hadoop Platform", *Hindawi Computational Intelligence and Neuroscience* (2018).
 - [8] Z Dou, M Song, K Gao, and Z Jiang, "Image Smoothing via Truncated Total Variation", *IEEE conference proceeding paper on computer vision* (2017).
 - [9] D Wang, "Extremely Optimized DRLSE Method and Its Application to Image Segmentation", *IEEE open access journal*, Vol. 7, pp. 119603-119619 (Sep. 2019).
 - [10] Z Wang and W Wang, "The research on edge detection algorithm of lane", Springer *EURASIP Journal on Image and Video Processing* (2018).
 - [11] M. Hammad, Y. Liu and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint," in *IEEE Access*, Vol. 7, pp. 26527-26542 (2019), doi: 10.1109/ACCESS.2018.2886573.
 - [12] Baby Sherin C and Mredhula L, "A Novel Method for Edge Detection in Images Based on Particle Swarm Optimization", IOP publishing, *Journal of Physics* (2017).
 - [13] Soni, Y. Improved and secure framework for existing e-Bazaar model in Rajasthan. *Journal of Information and Optimization Sciences*, 43(8), 1975-1985 (2022). <https://doi.org/doi.org/10.1080/02522667.2022.2111042>.