Received: May 6, 2020. Revised: July 8, 2020.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Secured Digital Handwritten Signature Prototype for Visually Impaired People

Mohamed Taha[1]* **Mazen M. Selim[1]** **Ahmed Yousry[1]**

[1]*Faculty of Computers and Artificial Intelligence, Computer Science Department, Benha University, Egypt*
* Corresponding author Email: mohamed.taha@fci.bu.edu.eg

Abstract: No doubt, Visually Impaired (VI) have trouble signing documents. They cannot identify their signatures and have their identification verified. Hence, some people may impersonate their identity. They may imitate their signatures in formal documents like contracts, money checks, and other vital documents, mainly in the governmental institutions. No clarified method can maintain these signatures. This paper presents a new prototype for securing VI people's signature using encryption techniques and data hiding methods. The proposed prototype uses the Least Significant Bit (LSB) algorithm for hiding some information, including the name of VI, the date, and the time of the signature. These data are encrypted using an improved, chaotic algorithm with a linear feedback shift register approach. Moreover, a QR code for each VI person is created and associated with the document. Both the signature and the QR code can be used to secure and validate the VI signature for a given document. A real signature dataset is constructed for evaluating the proposed prototype. The experimental results with respect to the real dataset and the Spanish signature dataset (MCYT-100) proved that the superiority of the proposed prototype.

Keywords: Chaotic algorithm, Digital signature, LSB, Encryption distance, Left shifting, Steganography.

1. Introduction

Throughout life, one has possibly used the telephone without thinking about it very much. However, if he is a visually impaired person, this pleasurable activity can become problematic. Reading and writing are taken for granted by most of us. However, if one has a low vision, the possibility that he can no longer read is the most significant problem in his life. Fortunately, many researchers provided many techniques for helping those people to learn everything. The assistive tools start from reading emails to getting the latest bestseller. Entertainment books, audiobooks, magnification tools, mobile applications, and a growing number of products allow VI to continue reading their morning papers and many other things. Although there are various reading tools available to visually impaired people, it is essential to know that any solution will require VI to learn reading differently.

Signature is one of the vital and broadly standard biometric modalities. It is the most common method used in different documents, including legal documents, financial transactions, contracts, etc. Nobody knows how many people cannot sign a document, or have problems doing so, but it is likely to number many thousands. A visually impaired person may never have had a signature. He will most likely have questions about his eyes and vision, as well as concerns about continuing to carry out his everyday life. One simple and straightforward solution is using signature guides. Typically, it is made of dark cardboard or metal template (or plastic), with a cutout area corresponding to space where the document or check is signed. It enables a VI person to sign on a dotted line. Some VI people prefer to have a signature stamp, while others ask someone to place their index finger on the line where they must sign. Signature guides are inexpensive and come in various sizes. VI people can keep them in the places they are most likely to use them, such as their home, office, or wallet. When the VI is ready to sign, he asks someone to put the window of the guide over the signature line, hold the guide in place, and sign in the area outlined by the window, as shown in Fig. 1.

Figure. 1 Examples of signature guides for an envelope and a check writing guide

Figure. 2 A snapshot of the proposed prototype

If somebody uses another person's document and deceits to be owner person, it is not easy to verify this document. Someone may copy one's signature into another document, improperly. However, in the digital signature, the criminal finds difficulty in doing that. A digital signature relates a digital sequence with an electronic document to simulate a handwritten signature on a printed paper document. This digital sequence ought to be thought-about like a written signature.

Digital Signature is a technique used to provide security for data through data privacy, integrity, and authenticity. Many encryption techniques are widely used, like RSA, AES, and DES. Besides, steganography techniques are used for hiding data in a carrier such as a digital image or a video. Least Significant Bit (LSB) [1] is one of the efficient techniques used for information hiding.

The number of VI people is large, may reach millions, as indicated by the World Health Organization (WHO) [2] and the LANCET Global Health (LGH) in 2017 [3]. So, there is an urgent need for a method that can keep the written signature of VI people secured and encrypted in a complicated way that prevents abuse from unauthorized people.

Governmental institutions and banks are struggling to find safe ways to obtain visually impaired signatures. Many methods have been introduced for preserving data over the internet, as well as the integrity of data. They are trying to make sure that the data that arrived at the receiver is the same as the one that was sent.

This paper presents an effective and robust prototype for securing a digital signature for visually impaired people. The proposed prototype uses the Least Significant Bit (LSB) algorithm for hiding some information, including the name of VI, the phone number, the date, and the time of the signature. These data are encrypted using an improved, chaotic algorithm with a linear feedback shift register approach. Also, a QR code for each VI person is generated and associated with the document. Hence, it is possible to verify the authenticity of the VI person using both the signature and the QR code. This scheme increases the complexity of uncovering the content of the hidden data of the signature. The proposed prototype has been implemented on an Android tablet. It supports freedom of movement and ease of use, which makes it very suitable for VI people. Fig. 2 shows a snapshot of the proposed prototype.

The main contributions of our work can be summarized as follows: A prototype for securing VI people's signature using encryption techniques and data hiding methods is proposed. An improved secure chaotic algorithm with a linear feedback shift register is proposed to protect VI signatures without any influence on the process of signature matching. The proposed prototype is tested using two datasets, and it achieves higher accuracy and lower Equal Error Rate (EER) comparing to its peers. A real dataset is self-collected and prepared, and it will be beneficial for researchers for further research.

The rest of the paper is organized as follows; Section 2 provides a literature review about the verification methods of a handwritten signature. Next, Section 3 presents the proposed work. Section 4 demonstrates the experimental results. Finally, Section 5 concludes the paper.

2. Related work

In the literature, many methods have been presented for preserving data privacy and integrity using digital handwritten signature.

Xia et al. [4] introduced a dynamic method of signatures verification that is applied to mobile phones. A key point for verifying signatures is to extract excellent distinguishing features. The extraction process includes four main steps: preprocessing, generation of attributes, truncation & quantization of attributes, and generation of features. First, their method divides a signature into multiple regions and extracts features from those different regions in addition to the global features extracted from the entire signature. The feature vector is a combination of both local and global features. A user template is built by averaging the feature vectors

whose elements are scaled by the feature-specific factors. Then, the similarity score of the test signature to the user template can be measured by Euclidean distance. The main drawback of this method is that it takes a long time for the classification process

Carbune et al. [5] developed an online handwriting recognition system. They used about 102 languages in 26 scripts from Google. The system is based on a qualified end-to-end neural network, replacing their old segment-and-decode system. The new system's accuracy in recognition is improved by 20–40 percent relative depending on the language while using both smaller and faster models. They encoded the touch inputs using a representation of the Bézier curve, which performs at least as well as raw touch inputs. However, the method has high complexity and a high error rate.

In most signature verification methods that are based on neural networks, the input signature image should be of fixed-size. However, signatures size varies actually in range among various users. By changing the network architecture using spatial pyramid pooling, Hafemann et al. in [6] tackled this problem by learning a fixed-size representation from variable-sized signatures. They also examine the influence of image resolution used for training and the effect of adapting the descriptions to new conditions of service. A limitation of this method is providing only offline verification for signatures.

Beresneva et al. [7] examined a few methods to extract the main information parameters of the handwritten signature, such as discrete Fourier and Radon transforms. They proved that the most perspective technique is discrete Wavelet transform. Also, they suggested using the methods of k-Nearest Neighbors and Random Forest because of their high accuracy in recognition. The main parameters of the signature are shape, size, pressure, velocity, etc. The accuracy of this method ranges from 60% to 95%. So, it is not stable and does not convenient for VI people. The researchers in [8-10] described a solution based on Convolutional Neural Network (CNN) using the TensorFlow library. The model is prepared with a dataset of signatures. The expectations are made as to whether a given signature is veritable or manufactured. These methods perform well, but there are not applicable for VI people and take a long time. So, it is not valuable for VI people.

In [11], Ruiz et al. suggested using a Siamese Neural Networks to assist in solving the offline handwritten signature confirmation issue with accidental imitations in a signer-independent context. Their method can be used on new signers without any more training required. Initially, they trained Siamese Neural Networks using GAVAB dataset signatures and different combinations of synthetic data. When mixing original and synthetic signatures for the preparation, the best verification results were obtained. This method performs only for offline verification of signatures.

Furthermore, Mersa et al. [12] proposed an Offline Signature Verification (OSV) system that includes two steps, learning representation and confirmation of the input signature. The signature images are then fed into a qualified Residual CNNs for the first step. The output representations are then utilized for training SVMs for the confirmation. They test their framework on three distinctive signature datasets, a Spanish signature dataset (MCYT), a Persian one (UTSig), and a manufactured dataset (GPDS-Synthetic). On the UTSIG, they accomplished a 9.80% Equal Error Rate (EER), which showed substantial enhancement over the finest EER within the writing, 17.45%. Their strategy outperformed state-of-the-arts by 6% on GPDS-Synthetic, achieving 6.81 %. On MCYT, EER of 3.98% was gotten, which is comparable to the finest already results.

Riesen et al. [13] presented a comprehensive comparison of two noticeable string matching algorithms: Dynamic Time Warping (DTW) and String Edit Distance (SED). They concluded that SED is more powerful than the widely used DTW, when the cost model is carefully adapted to the specific requirements of the application. A key limitation of this research is that it has a high error rate on the three benchmarking datasets.

In [14], a model for online signature verification based on user-dependent feature selection and Gaussian trapeze-shaped is presented. This method is computationally efficient since it works on a reduced subset of features. The model was thoroughly tested using widely accepted sets of data. Experimental results show that the model best achieves EER with all datasets.

Shariatmadari et al. [15] introduced a signer-dependent method for verifying signatures of signers through taken handwriting images. It is based on a one-class CNN approach that is learned through a hierarchical, coevolutionary neural network. They regard signature confirmation as a one-class issue, as in the real application scenario, forgeries are unaccessible. Their experiments show, in order to obtain better similarities between the genuine signatures, features of a lower level that can be extracted in the first layers are considered. Higher-level features which can be extracted in later layers are considered for discriminating genuine from forgery. The problem with this method is that it has a significant error rate.

Also, Toradmalle et al. [16] introduced a brief survey of the application of ECDSA and RSA on Hand-written signature verification using different viewpoints like time, security, and control. This method has a short time in getting results, but there are now attacks on the RSA algorithm without any improvements.

Fischer et al.

In [17], a framework based on a coordinate comparison of the basic neuromuscular strokes recognized within the handwriting is proposed. Taking under consideration the number of strokes, their similitude, and their timing, the string alters separate is utilized to determine a disparity degree for signature confirmation. The results of this method have a high error rate.

There is another method presented in [18]. It provides a signature verification using critical segments for securing mobile transactions. The EER of this method is less than 2 % but not clear.

3. Proposed prototype

Recently, considerable attention has been paid to developing tools to assist VI people in carrying out their daily activities smoothly and naturally. However, further work needs to be done to address many issues. Securing the VI signatures is one of these issues that has a growing interest in recent years. This paper presents a secured Digital Handwritten Signature Prototype for Visually Impaired people. The proposed prototype consists of two main phases: *signature generation and signature verification.*

3.1 Signature generation phase

Fig. 3 shows the block diagram of the *generation phase*. First, a tablet device is used to capture the VI signature, as shown in Fig. 4 (a). Each document that needs to be signed has different dimensions, such as a contract, bank check, or receipt. Hence, the captured signature image is then rescaled to match the area dedicated to the signature in the document.

After that, the prototype asks the operator to enter some personal data of the VI individual, such as *name* and *phone*, as shown in Fig. 4 (b). Also, the *date* and *time* stamps are identified automatically from the prototype. Moreover, a QR generator is used to provide a random QR code for each document signed by the VI person, as shown in Fig. 4 (c). All these data are then encrypted and embedded in the signature image, as shown in Fig. 4 (d). The Least Significant Bit (LSB) algorithm is used as a steganography technique to protect the VI signer information. All the VI data are stored in the prototype database. Then, the QR code and the

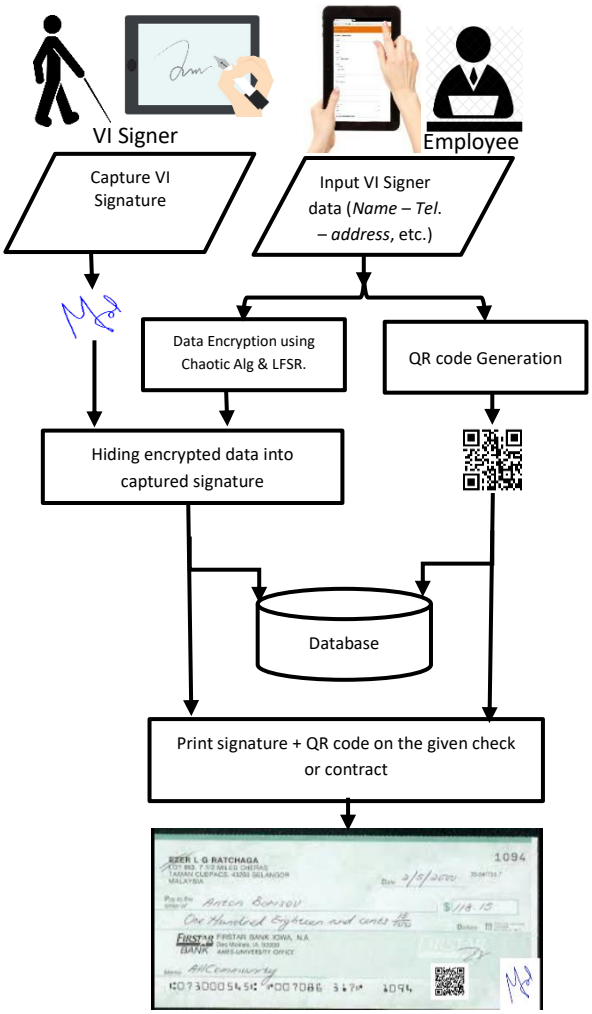
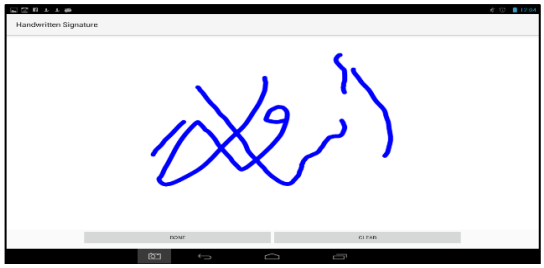


Figure. 3 The generation phase of the proposed prototype

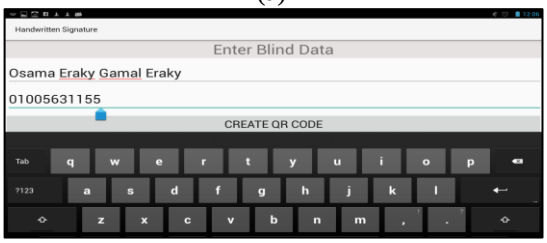
captured signature image are printed to the signature area of that document, as shown in Fig. 4 (e).

3.2 Signature verification phase

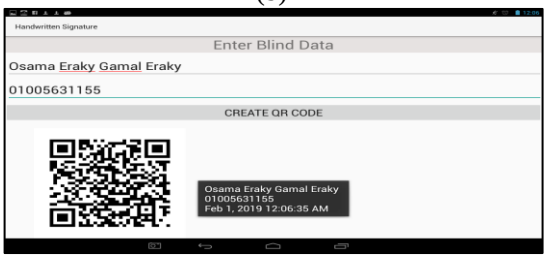
This phase is invoked when a signed document (e.g., a check or a contract) with the proposed prototype is presented to any governmental institute (e.g., a bank). This document needs to be verified against tampering. The QR code attached to the printed document is scanned by the tablet device that runs the proposed prototype, as shown in Fig. 4 (e). The QR data will be extracted and matched with the data stored in the prototype database, as shown in Fig. 4 (f). Also, the hidden encrypted data are extracted from the printed captured signature of the VI. To verify the authenticity of the signature, the extracted data are decrypted and matched with the stored data. Fig. 5 illustrates the steps of the s*ignature verification phase*.



(a)

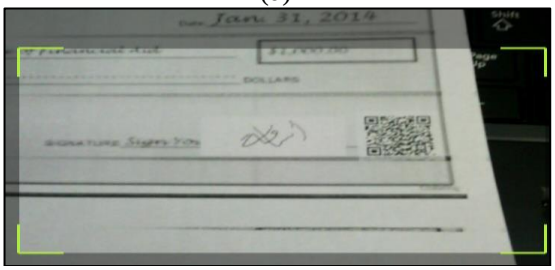


(b)

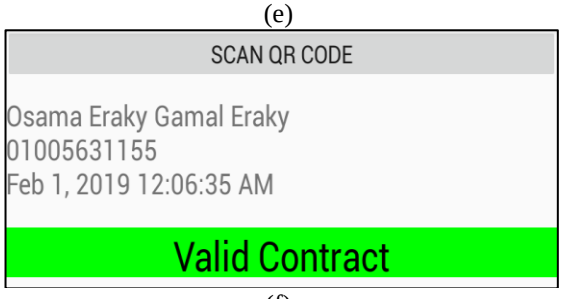


(c)

(d)



(e)



(f)

Figure. 4 Running the proposed prototype: (a) capture the signature, Input the personal data of the VI, (c) creating the QR code for the document, (d) The encrypted VI data printed on a check, (e) verifying the check by scanning the QR code, and (f) result of the validated data

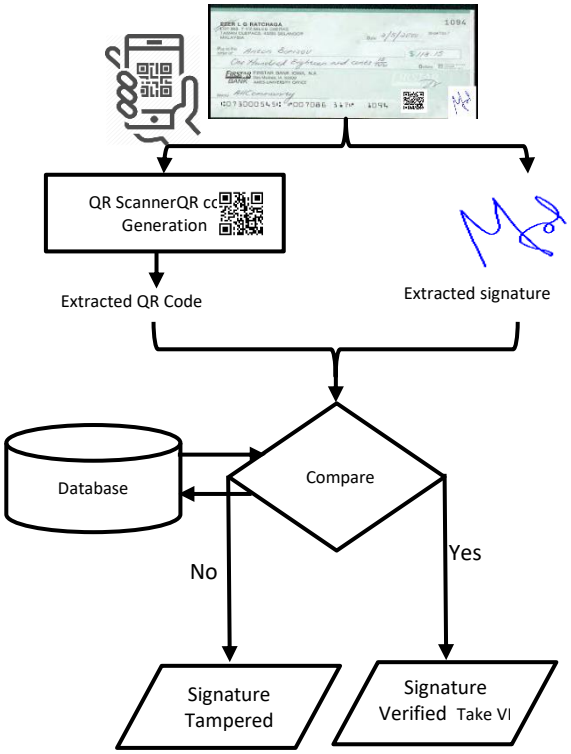


Figure. 5 The signature verification phase

3.3 Data encryption

The use of the Chaotic algorithm in cryptography has attracted much interest due to simple computation, and high speed. Security is the essential condition for authenticating the VI signature, and hence the use of chaotic maps must guarantee information security. In general, there is a set of factors that determine the level of security in any encryption algorithm. These factors include perceptual security, key sensitivity, key space, and its ability to respond to potential attacks. Therefore, a chaotic encryption algorithm must be secure in perception, have large key space, high key sensitivity, and resistant to attacks.

To achieve a high level of security in the prototype, we integrate the chaotic algorithm [19] along with the Linear Feedback Shift Register (LFSR) [20]. This integration makes the proposed prototype more secure and robust in the face of signature tampering attempts. LFSR ensures the data secrecy during long-distance transmission. The decoding of data encompasses inverting the feedback function or generating the binary sequence, which will assist in retrieving the data after some recombination operation.

The improved method of the Chaotic algorithm with the Linear Feedback Shift Register process is used to encrypt the VI data, including *name*, *phone*, *date*, and *time* of handwritten signature. The steps of the encryption algorithm are as follows:

1. Every character in the message is converted into an 8-bit binary representation.
2. Encryption keys are created using the logistic map of Eq. (1) where $key^{(i)}$ represents the present key.

$$Key^{(i)} = r * key^{(i-1)} (1- key^{(i-1)}) \quad (1)$$

3. Each key is converted into its binary 8-bits.
4. Every 8-bit binary ($key^{(i)}$) is XORed with every character binary 8-bits ($VD^{(i)}$) using Eq. (2).

$$X^{(i)} = VD^{(i)} \oplus key^{(I)} \quad (2)$$

5. The Linear Feedback Shift Register keys ($L\_key^{(i)}$) are calculated using Eq. (3), *LFSR_function* is explained in Fig. 6.

$$L\_key^{(i)} = LFSR\_function (Key^{(i)}) \quad (3)$$

6. The result of the LFSR keys is XORed with results from step 4 as shown in Eq. (4).

$$Y^{(i)} = L\_key^{(i)} \oplus X^{(I)} \quad (4)$$

The best value for Growth rate (r) is 3.8, according to the behavior shown in Fig. 6 [21]. The logistic map is robust in creating random keys. It is characterized by its ability to generate an infinite chaotic sequence of numbers. These numbers are used in the encryption algorithm. Comparing to usual congruential, periodic, random generators, the logistic random number generator is infinite, aperiodic, and not correlated [21].

Moreover, the integration of the chaotic algorithm and the LFSR provides an efficient method to convert the VI data into an encoded ciphertext, not easily predictable ensuring that the key value is irretrievable when data is attacked.

3.4 Data steganography

LSB [1] is a very well-known technique amongst steganography methods. In LSB, the lesser bits of cover image pixels are used to mask the hidden information. The conventional LSB technique is straightforward but not very useful. In some modified LSB schemes [22], a few bits from the most significant side decide the place where the secret bit is to be concealed, at least a considerable side.

To maximize the security of LSB steganography in the proposed protoype, the concept of LFSR is employed [20] as a random number generator. LFSR is a shift register where the input bit is a linear

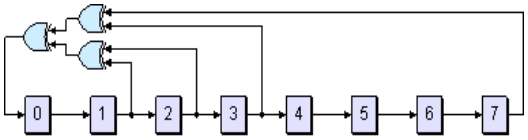


Figure. 6 The function of LFSR. Where 0 to 7 represent the 8-bit indexes that have a value of 0 or 1. The result of the final XOR process is used to take place the value of index 0, and the remaining bits are shifted to the right by one shift for the second iteration.

function of the previous state. The primary value of the LFSR is called a seed. The shift register operation is deterministic. If the current state is known, then the next sequence of values can be evaluated. An extensive series of random bits can be generated by LFSR having a well-chosen feedback function. The LFSR-generated bitstream is pseudo-random and also satisfies the requirements of cryptographic randomness. The shift register and feedback function are the two main parts of LFSR. A shift register's function is to move the register's contents in one direction to its neighboring locations so that one location on the other end is empty. The place remains empty if no new content is entered into the registry. The new content is created via a linear function. The inputs are the contents of positions filled in. There is an exception in LFSR, if all the contents of the shift register are zeros, then it is impossible to produce the next state.

In this step, the encrypted data will be embedded in the signature image using the Least Significant Bit (LSB) method [22]. This method uses the least bit for storing critical data in a binary form where the least significant bit of pixels of the signature image is replaced with data bits. These binary data do not affect the image details significantly. The LSB technique is very efficient due to its simplicity and its ability not to be noticeable or suspicious.

3.5 Extracting hidden data

At this stage, the inverse of all previous operations is applied. The extraction procedure of the LSB steganography technique is used to extract the secret data from the signature image. The result of this process is encrypted VI data. These data are then decrypted using the inverse process of the chaotic algorithm and linear feedback shift register. Hence, we will again obtain the original data before encryption and steganography.

3.6 QR code generation and scanning

The QR code is employed in the proposed prototype to verify any formal document signed by

VI people against tampering. This process is crucial for printed documents only. The QR code generator is implemented to provide a random QR code for every formal document (e.g., check or contract). All the VI signer data, such as *name* and *address*, are entered by the employee using the proposed prototype. Also, the *time* and *date* stamp are recorded automatically by the prototype. These data are encrypted and embedded in the QR code for security issues. Also, they are saved in the prototype database to be used later in the verification process. The generated QR code is printed on the document with the secured signature. QR scanner is used for the verification process by scanning the QR code attached to the printed document and matching the extracted data with the stored data in the prototype database. If the extracted data is the same as in the database, then the printed document is valid and accepted.

4. Experiment and results

4.1 Experiment setup

The proposed prototype is implemented using a SICO (ST-10-3G) tablet. The device has 1 GB RAM with an Android system. The proposed prototype is tested using two datasets: our own real VI dataset, and the MCYT-100 dataset [23].

First, the signature of the visually impaired is taken using the electronic pen on the tablet screen. Second, the captured signature is rescaled to match the document where the signature will be printed. Then, the personal data of the signer (such as name, phone number, etc.) is entered into the system. In addition, the date and the time stamps are automatically recorded. These data are then encrypted using our improved chaotic algorithm with LFSR. Finally, this encrypted data are concealed in the signature image.

Moreover, a QR code is generated for every document depending on the VI personal data and the document id. These data are encrypted and embedded in the QR code for security issues. When creating the QR code, the data of VI is also saved in the database of the prototype to use it later in the verifying process.

Fig. 7 shows an example of a bank check attached with a sample of a handwritten digital signature and the QR code of a specified VI person. This check is encrypted and can only be decrypted using the proposed prototype.

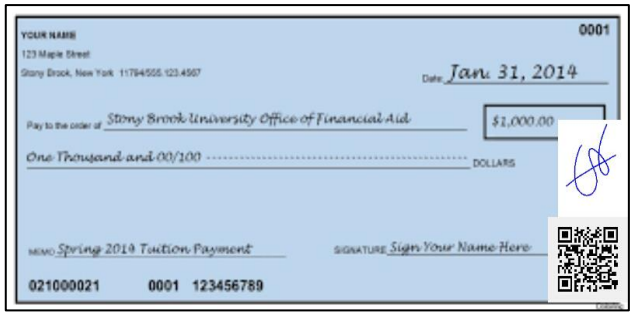


Figure. 7 A check with a signature and QR

4.2 Performance and comparison

To evaluate the performance of the proposed work, two experiments are conducted. In the first one, we used our dataset of real VI people. Some of them have low vision, and others are blind. The second experiment was conducted on the Spanish signature dataset (MCYT-100) taken by a WACOM pen tablet [23].

4.2.1. Experiment one (our real dataset)

Unfortunately, we did not find datasets available for Arabic signatures to be used in evaluating the performance of the proposed prototype, so we had to build our dataset. In order to achieve this goal, a group of sixteen Egyptian volunteers living in one of the care centers for the visually impaired was involved. Ten genuine signatures have been taken from each one with different sizes and styles. Hence, the total number of the acquired genuine signatures is 160 (see Fig. 8). Fig. 9 shows samples of collected signatures from VI people. For each genuine signature, another forged signature has been created, making 160 forged signatures as a total.

Table 1 shows the confusion matrix of running the proposed prototype with our real dataset that contains 160 genuine signatures plus 160 other forged signatures. The numbers in the table represent True Positive (TP), False Negative (FN), False positive (FP), and True Negative (TN), respectively. To measure the performance of the proposed prototype, precision and recall metrics are calculated using the following equations:

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (5)$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (6)$$

The proposed prototype achieves a precision equal to 96.9% and a recall equal to 98.1%. These results indicate the high performance of the proposed prototype.

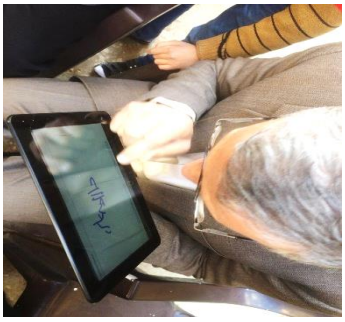


Figure. 8 Visually impaired person signs on the tablet screen

Figure. 9 Samples of collected handwritten signatures

Table 1. Confusion matrix of running the proposed prototype with our real dataset

		Predicted	
		Genuine	Forged
Actual	Genuine	TP 157	FN 3
	Forged	FP 5	TN 155

4.2.2. Experiment two (MCYT-100 dataset)

In this experiment, the proposed prototype is tested against the Spanish signature dataset (MCYT-100), a benchmark dataset. It can be found in (http: //atvs.ii.uam.es/atvs/mcyt75so.html). This dataset consists of 15 genuine and 15 forged signatures from 100 people. The Receiver Operating Curve (ROC) in Fig. 10 summarizes the results of the proposed prototype at all classification limits. Notably, the ROC curve plots the False Positive Rate (FPR) on the X-axis and the True Positive Rate (TPR) on the Y-axis, where FPR can be calculated using Eq. (7) and TPR can be calculated according to Eq. (8).

$$\text{FPR (1- specifity)} = \frac{FP}{TN+FP} \tag{7}$$

$$\text{TPR (sensitifity)} = \frac{TP}{TP+FN} \tag{8}$$

The performance is calculated in terms of the Equal Error Rate. The EER is the point within the Detection Error Tradeoff (DET) curve, where the false acceptance rate rises to the false rejection rate. The proposed work achieved an outstanding EER value of 0.16 % and Area Under the ROC Curve (AUROC) of 99.3 %.

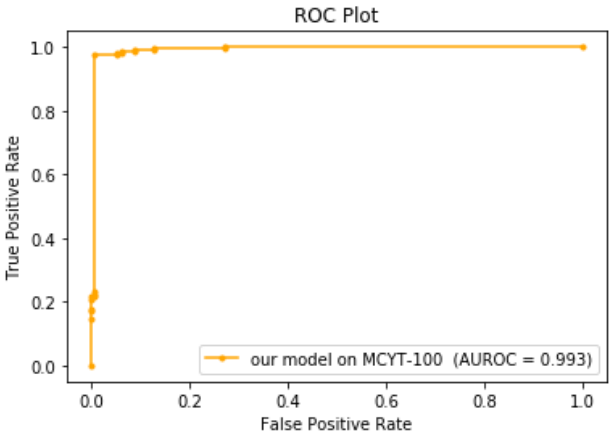


Figure. 10 ROC curve when testing the proposed work on MYCIT 100 dataset

Table 2. Comparison between previous work and the proposed prototype using MYCIT dataset

Systems	**AUROC**	EER %
Combinational features and KNN [4]	-	0.29
Offline hand-written signatures [6]	-	0.19
Siamese Neural Networks [11]	98.6	2.06
Transfer Learning Approach [12]	-	3.98
String edit distance [13]	-	4.20
Kinematic Theory [17]	-	3.83
Critical Segments [18]	-	2
Proposed work	**99.3**	**0.16**

A comparison is made between the proposed prototype and its counterparts [4, 6, 11-13, 17, 18] for the MCYT-100 dataset. Table 2 shows the comparative results with respect to EER and AUROC metrics. As it can be seen from the table, the proposed prototype outperforms the other techniques. This is because it employs more than one technique to secure the signature of the VI people. It provides an improved secure chaotic algorithm with a linear feedback shift register. Besides, it exploits the Least Significant Bit algorithm to conceal some crucial data in the signature image. In addition, it uses QR technology to authenticate both the signature and the document.

5. Conclusion and future work

The visually impaired people find it great challenging to sign documents in such a way that everyone can sign. Moreover, they fear that fraudsters may misuse their signatures or that their signature will be forged. This paper has introduced a prototype for securing digital signatures for visually

impaired people. An improved secure chaotic algorithm with a linear feedback shift register is proposed to protect VI signatures. The proposed prototype uses the Least Significant Bit (LSB) algorithm for embedding some personal information of VI, including the name, the phone number, the date, and the time of the signature. Also, a QR code for each VI person is generated and associated with the document. Therefore, it is possible to verify the validity of authentic signatures, and no one can forge the signatures of new documents. The proposed prototype is tested using two datasets, and it achieves higher accuracy and lower Equal Error Rate (EER) comparing to its counterparts.

Future work should concentrate on employing deep learning techniques for the classification process. Also, our results are promising and should be validated by larger sample size.

Conflicts of Interest

We declare no conflict of interest.

Author Contributions

Mohamed Taha, Mazen M. Selim, and Ahmed Yousry contributed to the design and implementation of the research to the analysis of the results and the writing of the manuscript.

Acknowledgments

The authors would like to express their gratitude to the Egyptian Al-Eradah Association for Special Needs Care, which has provided support and help for the research through the participation of sixteen visually impaired and blind individuals as volunteers to try and test the proposed prototype.

References

[1] C. Zhao, W. Ma, T. Yan, and Y. Sun, "Linear Complexity of Least Significant Bit of Polynomial Quotients", *Chinese J. Electron.*, Vol. 26, No. 3, pp. 573–578, 2017.

[2] D. Pascolini and S. P. Mariotti, "Global Estimates of Visual Impairment: 2010", *Br. J. Ophthalmol.*, Vol. 96, No. 5, pp. 614–618, 2012.

[3] R. Bourne, F. Seth, B. Tasanee, and C. Maria, "Magnitude, Temporal Trends, and Projections of the Global Prevalence of Blindness and Distance and Near Vision Impairment: a Systematic Review and Meta-Analysis", *Lancet Glob. Heal.*, Vol. 5, No. 9, pp. 888–897, 2017.

[4] Z. Xia, T. Shi, N. N. Xiong, X. Sun, and B. Jeon, "A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure KNN", *IEEE Access*, Vol. 6, No. c, pp. 46695–46705, 2018.

[5] V. Carbune, G. Pedro, D. Thomas, R. Henry A, D. Alexander, and C.Marcos, "Fast Multi-Language LSTM-based Online Handwriting Recognition", *Int. J. Doc. Anal. Recognit.*, 2020.

[6] L. G. Hafemann, L. S. Oliveira, and R. Sabourin, "Fixed-sized Representation Learning from Offline Handwritten Signatures of Different Sizes," *Int. J. Doc. Anal. Recognit.*, Vol. 21, No. 3, pp. 219–232, 2018.

[7] A. Beresneva, A. Epishkina, and D. Shingalova, "Handwritten Signature Attributes for its Verification", In: *Proc. of 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2018*, Vol. 2018-Janua, pp. 1477–1480, 2018.

[8] S. Jerome Gideon, A. Kandulna, A. A. Kujur, A. Diana, and K. Raimond, "Handwritten Signature Forgery Detection Using Convolutional Neural Networks", *Procedia Comput. Sci.*, Vol. 143, pp. 978–987, 2018.

[9] R. D. Rai and J. S. Lather, "Handwritten Signature Verification Using TensorFlow", In: *Proc. of 2018 3rd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2018*, pp. 2012–2015, 2018.

[10] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning Features for Offline Handwritten Signature Verification Using Deep Convolutional Neural Networks", *Pattern Recognit.*, Vol. 70, pp. 163–176, 2017.

[11] V. Ruiz, I. Linares, A. Sanchez, and J. F. Velez, "Offline Handwritten Signature Verification Using Compositional Synthetic Generation of Signatures and Siamese Neural Networks", *Neurocomputing*, Vol. 374, pp. 30–41, 2020.

[12] O. Mersa, F. Etaati, S. Masoudnia, and B. N. Araabi, "Learning Representations from Persian Handwriting for Offline Signature Verification, a Deep Transfer Learning Approach", In: *Proc. of 4th Int. Conf. Pattern Recognit. Image Anal. IPRIA 2019*, pp. 268–273, 2019.

[13] K. Riesen and R. Schmidt, "Online Signature Verification based on String Edit Distance", *Int. J. Doc. Anal. Recognit.*, Vol. 22, No. 1, pp. 41–54, 2019.

[14] V. Chandra Sekhar, M. Prerana, D. S. Guru, and V. Pulabaigari, "Online Signature Verification Based on Writer Specific Feature Selection and Fuzzy Similarity Measure", *CoRR*, Vol. abs/1905.0, 2019.

[15] S. Shariatmadari, S. Emadi, and Y. Akbari, "Patch-based Offline Signature Verification Using One-Class Hierarchical Deep Learning",

Int. J. Doc. Anal. Recognit., Vol. 22, No. 4, pp. 375–385, 2019.

[16] D. Toradmalle, R. Singh, H. Shastri, N. Naik, and V. Panchidi, "Prominence Of ECDSA Over RSA Digital Signature Algorithm", In: *Proc. of Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2018*, pp. 253–257, 2019.

[17] A. Fischer and R. Plamondon, "Signature Verification Based on the Kinematic Theory of Rapid Human Movements", *IEEE Trans. Human-Machine Syst.*, Vol. 47, No. 2, pp. 169–180, 2017.

[18] Y. Ren, C. Wang, Y. Chen, M. C. Chuah, and J. Yang, "Signature Verification Using Critical Segments for Securing Mobile Transactions", *IEEE Trans. Mob. Comput.*, Vol. 19, No. 3, pp. 724–739, 2020.

[19] L. Juan, F. Yong, and Y. Xuqiang, "Discrete Chaotic Based 3D Image Encryption Scheme", *2009 Symp. Photonics Optoelectron. SOPO 2009*, pp. 1–4, 2009.

[20] C. Maxfield, "Linear Feedback Shift Registers", *Des. Maximus Unleashed*, No. 19, pp. 219–232, 1998.

[21] Ashish, J. Cao, and R. Chugh, "Chaotic Behavior of Logistic Map in Superior Orbit and an Improved Chaos-Based Traffic Control Model", *Nonlinear Dyn.*, Vol. 94, No. 2, pp. 959–975, 2018.

[22] I. G. Wiryawan, Sariyasa, and I. G. A. Gunadi, "Steganography Based on Least Significant Bit Method was Designed for Digital Image with Lossless Compression Technique", In: *Proc. of 2018 Int. Conf. Signals Syst. ICSigSys 2018*, pp. 98–102, 2018.

[23] L. Hollink, G. P. Nguyen, D. C. Koelma, A. T. Schreiber, and M. Worring, "Assessing User Behaviour in News Video Retrieval", *Inf. Syst. J.*, Vol. 152, No. 6, pp. 911–918, 2005.