

Received May 18, 2019, accepted May 29, 2019, date of publication June 5, 2019, date of current version June 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920858

Developing a Visual Cryptography Tool for Arabic Text

SULIMAN A. ALSUHIBANY 

Computer Science Department, College of Computer, Qassim University, Buridah 51951, Saudi Arabia

e-mail: salsuhibany@qu.edu.sa

The author gratefully acknowledges Qassim University, represented by the Deanship of Scientific Research, on the material support for this research under the number (5077-coc-2018-1-14-S) during the academic year 1439 AH/2018 AD.

ABSTRACT Over the years, cryptography has been used to encrypt secret data. A new version of cryptography, entitled visual cryptography (VC), has been introduced. This approach is a simple and secure way to allow the secret sharing of images without any cryptographic computations or the use of encryption or decryption keys. Although various studies have been undertaken with regard to improving the VC technique, there has not yet been a study attempting to improve the VC technique for Arabic text although there are thousands of websites that provide services in Arabic serving countries in which Arabic is spoken as a first language. This paper, therefore, develops a tool that can encrypt/decrypt images of Arabic text using the VC approach. We experimentally evaluate the usability aspect. The results indicate the general suitability of the developed tool. This tool sheds light in designing practical tools for electronic voting, anti-phishing, Captcha, watermarking, biometric privacy, online payment systems, and digital signature in the Arabic environment.

INDEX TERMS Arabic language, experimentation, security, visual cryptography.

I. INTRODUCTION

Over the years, cryptography has been used to encrypt secret data. A new version of cryptography was introduced by Naor and Shamir [1] entitled visual cryptography (VC). They define it as a simple and secure way to allow the secret sharing of images without any cryptographic computations and without using encryption or decryption keys. The main idea of VC is to divide the image into shares; when these shares are combined, the image is restored to the original; otherwise there is no result. Interestingly, the decryption process in VC is entirely based on the human visual system.

There are many differences between the English and Arabic languages. For example, English is a Germanic language from the Indo-European language family, while Arabic is a Semitic language belonging to the Afroalphabet language family [9]. Besides, English is written from left to right, whereas Arabic is written from right to left. Moreover, Arabic letters are connected when written, both in printed and handwritten text. Additionally, there are a large number of Arabic-speaking Internet users (around 50.3% Internet penetration in 2019, out of 421 million Arabs) [12], and it has

been empirically shown in [8] that when a website has been originally conceived in the native language of the user, then the observed usability is increased. Accordingly, although many studies have been done in order to improve the VC technique, there has not yet been a study aimed at improving the VC technique for Arabic text. Thus, this paper aims to develop a tool that encrypts/decrypts Arabic text using the VC technique.

In this paper, we have developed an Arabic VC tool using a website that allows users to decrypt an Arabic text. Furthermore, we experimentally evaluate the developed tool by conducting an experiment with five random encrypted Arabic texts, asking a group of sixty-four subjects to decrypt them. By analyzing this group, the time required for stacking shares over each other and recognizing the text was interesting. Furthermore, the success rate in terms of recognizing the decrypted text was more than 63%, and the satisfaction results point generally to the suitability of the developed tool.

This is a very encouraging result for this line of research, indicating that the tool merits further study. Moreover, this tool sheds light in designing practical tools for electronic voting, anti-phishing, Captcha, watermarking, biometric privacy, online payment systems and digital signature in the Arabic environment. Consequently, this research will serve

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

as a basis for future studies to enhance the proposed tool in terms of overcoming the limitations and applying it in a range of applications.

The rest of this paper is organized as follows. Section 2 discusses related works. An overview with regard to the Arabic language is given in Section 3. Section 4 explains the developed Arabic VC tool. Section 5 describes the experimental study, and its results are presented and discussed in Section 6. Section 7 concludes the paper.

II. RELATED WORKS

To the best our knowledge, this work is the first of its kind to encrypt Arabic text using the visual cryptography (VC) method. This section, therefore, highlights the VC method in terms of its mechanisms and applications.

In 1994, a new version of cryptography was introduced by Naor and Shamir [1] entitled a visual cryptography (VC) or visual cryptography scheme (VCS). They defined it as a simple and secure way to allow the secret sharing of images without any cryptographic computations nor requiring the use of encryption or decryption keys. The main idea of this VCS is to divide an image into a set of shares. When these shares are recombined, the image is returned to the original; otherwise no result will be shown. Moreover, VC is used to encrypt the image based on the human visual system. This means that it can be readable by human users as they can recognize the recovered secret with their visual system, without the intervention of machines.

Different VC schemes have been compared in [3] in terms of image format, binary, gray, and colored image. The first scheme [1], in 1994, used a coding table to generate the shares, while the latest scheme [13], in 2014, used a hierarchical VC. These schemes have been utilized in numerous applications such as biometric privacy, online payment systems, anti-phishing frameworks, and authentication based on signature, as summarized in [4]. Moreover, a very recent work [7] reviewed various visual cryptographic schemes based on different pieces of research related to this area, and cited the relevant literature. Furthermore, different VC schemes have been compared in terms of various performance criteria such as pixel expansion, visual quality and security. This study concluded that every day new VC techniques are being developed; hence the identification of secure and good VC schemes will always be of value.

Another study [5] proposed a letter-based VC scheme where pixels are replaced by letters for the share image. The results showed that this proposal satisfies the security conditions.

Although our work does not involve the development of a new VC technique, it has developed a VC tool for use with the Arabic language, and evaluates its performance in terms of efficiency, effectiveness and satisfaction.

III. ARABIC LANGUAGE: AN OVERVIEW

This section explains the characteristics of the Arabic language in terms of writing direction and shapes. Specifically,

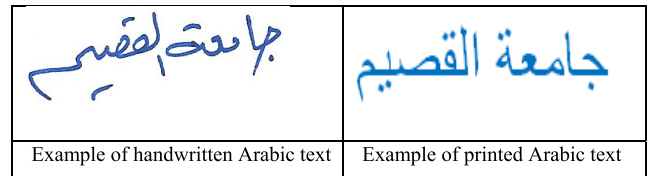


FIGURE 1. Arabic handwritten and printed text samples.

Arabic is a Semitic language belonging to the Afroalphabet language family [9]. Moreover, the Arabic language has 28 basic letters that can be written using 15 primary strokes, and they only differ in terms of the number or position of the letters' dots. Arabic writing runs from right to left, and letters are connected when written, both in printed and handwritten texts, as shown in Figure 1.

Generally speaking, Arabic letters are context-sensitive, where a single letter can be written in up to four different contextual-shapes depending on its position in the word. For instance, the form of the letter Meem can be either "م", "مم", or "مـ" where it can be a single letter, at the end of the word, between two letters, or at the beginning of the word, respectively. Moreover, several Arabic characters have similar shapes as follows:

(ف، ق)، (ر، ز، و)، (د، ذ)، (ط، ظ)، (ع، غ)، (ص، ض)، (ج، ح، خ)،
(ب، ت، ث، ن)

In contrast to Latin script, there are various features in Arabic script. For example, a lack of space between letters is one of these features as letters are not usually separated by a space. Moreover, diacritics are used in Arabic text, e.g. Shadda, Maddah, Hamza, Tanween. In addition, when typing Arabic text, there can be overlapping between characters in terms of space, e.g. "وا" in which "ا" overlaps with "و".

IV. ARABIC VISUAL CRYPTOGRAPHY TOOL

















This section explains the developed tool in terms of the VC algorithm used and the graphical user interface (GUI).

A. VC SCHEMES IN USE: AN OVERVIEW

There are numerous types of VC schemes. For example, there is the k-out-of-n scheme, in which k refers to the number of shares that should be stacked to decrypt the secret image, and n refers to the shares that will be produced, 2-out-of-2 and n-out-of-n [10]. In this paper, the 2-out-of-2 scheme is selected due to its transparency in terms of describing the idea of VC and the security level that can be provided.

In order to explain the construction of the 2-out-of-2 scheme, suppose that we have a binary secret image S that contains m pixels. This image is then divided into two shares: S₁ and S₂. These shares contain the same pixels as S (i.e. each pixel in the S is divided into two pixels). This is illustrated in Table 1. For example, if the pixel in S is white, then one row from the first two rows of Table 1 is randomly chosen. Likewise, if the pixel in S is black, then one row from the last two rows of Table 1 is randomly chosen.

TABLE 1. 2-Out-Of-2 scheme with sub-pixel layout.

Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
	0			
	0			
	1			
	1			

In order to analyse the security of this chosen scheme, one of the two pixel patterns (white or black) from Table 1 is randomly selected for S_1 and S_2 . Since this selection is random, these shares include the same number of black and white pixels. Accordingly, by inspecting a single share, it is impossible to recognize the secret pixel as being white or black. This scheme thus provides a good level of security.

Generally speaking, 1 represents the white pixel in the VC, while 0 represents the black pixel. For the selected scheme, the basis matrices S^0 and S^1 are designed as follows [11]:

$$S^0 \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad S^1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The relative difference α and contrast β for the above basic matrices can be computed as $\alpha = 1/2$ and $\beta = 1$.

There are two collections of matrices: C_0 for encoding white pixels, and C_1 for encoding black pixels. Based on this, assume the following two collections of matrices: $C_0 = \{\pi(S^0)\}$ and $C_1 = \{\pi(S^1)\}$ where $\pi(S^0)$ and $\pi(S^1)$ represent the collection of all matrices achieved by permuting the columns of matrices S^0 and S^1 , respectively. That is:

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \quad \text{and} \quad C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

In order to share a white pixel, one of the matrices in C_0 is randomly selected, whereas one of the matrices in C_1 is randomly selected for sharing a black pixel. Therefore, share 1 (S_1) is represented by the first row of the chosen matrices, whilst share 2 (S_2) is represented by the second row.

In this chosen scheme, a distortion problem can occur. That is, for every pixel for the original image, two sub-pixels are encoded and placed on each share, either horizontally or vertically. Therefore, the shares have a size of $s \times 2s$ in the event that the size of the secret image is $s \times s$. This distortion issue has been solved using square pixel expansion, and more details can be found in [11]. In this paper, however, this distortion is not eliminated intentionally to evaluate the accuracy of the decryption. Not only this, but it might also be exploited as a feature in some possible security applications such as CAPTCHAs.

B. THE ALGORITHM DEVELOPED FOR ARABIC VC

This section highlights the technical side of the algorithm developed for Arabic text based on the VC scheme used, in which the Java programming language is used for the implementation.

Five functions have been developed for encrypting and decrypting an Arabic text using the selected VC scheme: set up, create text image, draw, encryption and decryption functions.

First of all, a set up function sets the image mode and canvas size. It also sets the location from which the shape is drawn, and sets the background color to white. Finally, it calls the *createTextImage()* function to create the image and embed the Arabic text.

The create text image function implements a default parameter for its argument *my_text* in the event that it is the first call to this function, or the users did not enter a string. It then resets the checks used to verify the image that has previously been encrypted, as a new image will be created. It then creates the image using the *createGraphics()* class, and sets the background and fill color. Moreover, it writes the Arabic text within the image and chooses a random position for the text inside the image.

The draw function handles the drawing and movement of the text if it is not encrypted. Not only this, but it also handles the drawing and movement of each share that is created. Furthermore, it gives feedback (i.e. success or fail) to the user when the images are exactly stacked over each other.

The decryption function generally defines an x, y position for each share. Based on these defined positions, it creates two shares twice the size of the original image in an array called *shares*. Then, it reads each pixel in the original image using nested loops. The function *get* retrieves the value of a specific pixel in a specific location. After this, it selects a random four pixel pattern for each pixel in the original image, and adds the pattern to the first share. If the original pixel is white, then the second share will have the same pattern. On the other hand, if the original pixel, the value returned from calling the function *get*, is black, then the second share will have the complement four pixel pattern. Each loop assigns four pixels for the first share and another four for the second share. The nested loops are terminated when the last pixel in the original image is reached. The *updatePixels()* function applies the changes made in the nested loops.

Finally, the *decrypt()* function allows the user to place the shares over each other by setting the same coordinates for both of them.

Based on the aforementioned description, the process of the algorithm is briefly summarized in the following steps:

- Create an image with specific dimensions,
- Read an Arabic string from a predetermined string,
- Embed the Arabic text string within the image,
- Read the image pixel by pixel as follows:
 - For the first share, choose a random four pixel pattern from the already defined patterns,
 - For the second share:
 - If the original pixel is white
 - Use the same four pixel patterns that were used in the first share

- Otherwise, choose the complement of the random pattern chosen in the first share
 - Make the white pixels always transparent,
 - Repeat the above for all the pixels in the image
- Each of the shares will be twice the size of the original image
- To get the original image, the user must stack the two shares exactly over each other.

C. GRAPHICAL USER INTERFACE

We have developed a website that shows the encrypted shares, and allows the user to undertake the decryption process. Figure 2 shows the encrypted shares before decryption, while Figure 3 shows the shares after decryption.



FIGURE 2. Showing the encrypted shares before the decryption.



FIGURE 3. Showing the encrypted shares after the decryption.

In these figures, in addition to the shares, we show the status of the decryption and a box to be filled with the decrypted text. In terms of the status of the decryption, it uses a green color when the decryption is done correctly, while a red color is used otherwise. Also, filling the box with the decrypted text allows us to verify the recognized text with the generated one. This will be explained in the following section.

V. EXPERIMENTAL STUDY

The aim of this experimental study is to evaluate the usability of the proposed Arabic VC tool. The following describes specific details of the experimental setup and procedure.

A. SETUP

The experiment involves a number of subjects; thus the design, text, participants, system and survey are described in this section.

1) DESIGN

We performed a within-subject lab study to evaluate the usability aspect of the proposed tool. In our study, we focus on the effects of using the VC with Arabic text in terms of efficiency, effectiveness, and satisfaction.

2) TEXT

The Arabic text used is predefined as random dictionary-based words that are shown in each request. For the purposes of our experiment, five random dictionary-based words are used for each participant.

3) PARTICIPANTS

We recruited sixty four participants (aged 21–32 years) from our campus population. The majority of participants had a Computer Science background.

4) SYSTEM

We developed a website using PHP language which is connected to a mysql database in order to record all answers.

5) SURVEY

We deployed an online survey using Google form. The survey consists of 3 questions, two of them are ranked on a 5-point Likert scale: Strongly Agree, Agree, neither agree nor disagree, Disagree and Strongly Disagree. These 3 questions are as follows. 1) Have you ever heard about VC before? 2) After using the proposed Arabic VC tool, do you think this tool is generally easy to use? 3) By using the proposed Arabic VC tool, do you think this tool might make decryption easy? At the end, the user can add any comments or suggestions. Therefore, this survey reflects user satisfaction.

B. PROCEDURE

The way that we ran the experiment is described, i.e. instructions to subject, usability procedures, and collected data.

1) DESIGN

Subjects were instructed that there is an Arabic VC tool that needs to be evaluated in terms of its usability aspects. The subjects were instructed that there is only one session for evaluating the usability of the tool. Subjects were asked to provide feedback regarding the proposed Arabic VC tool through a survey provided by the researcher.

2) USABILITY EXPERIMENT PROCEDURE

We assessed the usability of the proposed Arabic VC tool with a consideration of quantitative and qualitative metrics. The proposed tool's efficiency is measured by the time required for stacking shares over each other and recognizing the text;

to measure the time taken, we implemented a function in which the time taken is recorded. Moreover, the effectiveness is also assessed in terms of the success of recognizing the decrypted text by verifying the submitted recognized text with the generated one. In addition to these quantitative usability results, qualitative usability results are collected via a survey, which provides qualitative data on the user's satisfaction, based on participants rating the tool using a 5-point Likert scale, as explained previously.

3) COLLECTED DATA

The time required for stacking shares over each other and recognizing the text is recorded. Moreover, the text recognized after the decryption is recorded. Additionally, the users' satisfaction is collected.

VI. RESULTS AND DISCUSSION

This section shows the results of testing the efficiency, effectiveness, and satisfaction of the proposed tool.

A. THE EFFICIENCY

The time required for stacking shares over each other and recognizing the text is shown in Figure 4. We can see that the average time required for stacking shares over each other and recognizing the first shown encrypted text was highest at 17.8 seconds. On the other hand, the average time required for stacking shares over each other and recognizing the last shown encrypted text was the lowest at 14.5 seconds.

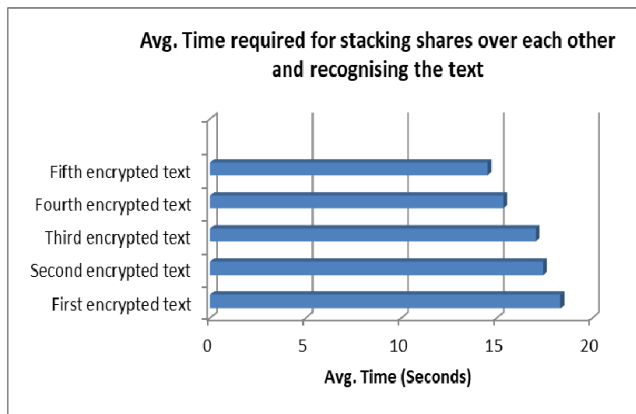


FIGURE 4. The average time required for staking shares over each other and recognizing the text.

It is interesting to note that a learning acquisition process is clearly observed in that the users have taken a long time to decrypt and recognize the first encrypted text, while the time is gradually decreased until we reach the fifth encrypted text. This may indicate that the usability of the developed tool can be improved with use. Furthermore, the results of the first question in the satisfaction section may support this observation, as most users had not had any experience of using the VC technique.

As mentioned previously, since this developed tool is the first of its kind to encrypt Arabic text using the visual

cryptography (VC) method, we could not compare this result with others.

B. THE EFFECTIVENESS

The success in terms of recognizing the decrypted text correctly is shown in Figure 5. This is done by verifying the submitted recognized text with the generated one. Interestingly, 65% of the decrypted texts were correctly recognized, while 35% were not correctly recognized.

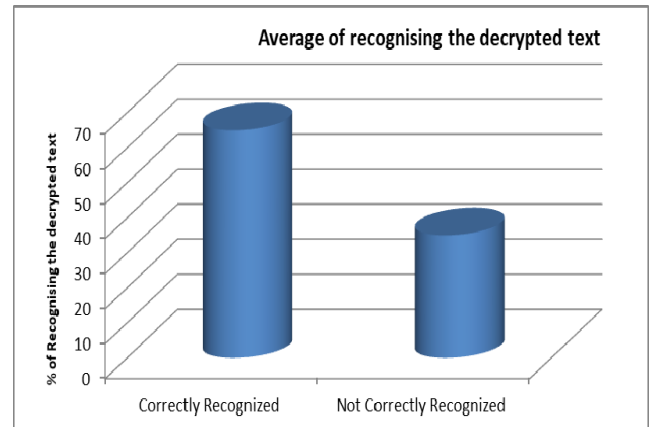


FIGURE 5. The average of recognizing the decrypted text.

There are several possible explanations for the not correctly recognized result. Firstly, since several Arabic characters have similar shapes, e.g. {ح, ج, ح}, {ب, ت, ث, ن, ي}, {ع, غ}, {ط, ظ}, {د, ذ, ر, ز, و}, {ف, ق} a confusion with regard to recognizing them can occur. For example, Table 2 shows a set of confusing characters that have been reported by the participants. Moreover, the background of the decrypted text may cause some difficulty in terms of recognizing the text, especially with characters that have similar shapes. This issue has been solved in [11] by using square pixel expansion, but we intentionally would like to evaluate the usability of the developed tool with regard to this issue. However, further research may be conducted to optimize the generation of the text then evaluating the

TABLE 2. A set of confusing characters.

Sample	Confusion
	The second character, from the right, is it "ف" or "ق"
	The fifth character, from the right, is it "ن" or "ت"
	The third character, from the right, is it "ث" or "ت"
	The second character, from the right, is it "ف" or "ق"

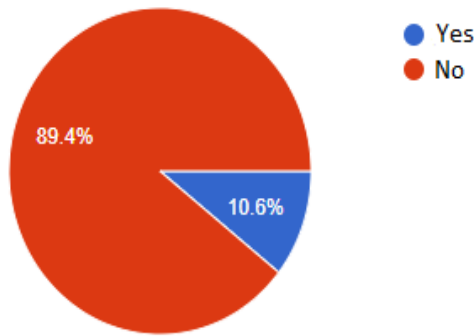


FIGURE 6. The result of the first question: Have you ever heard about VC before?

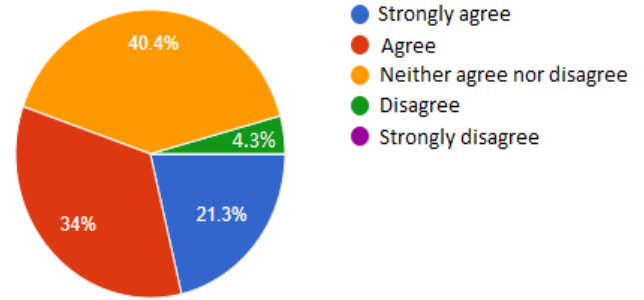


FIGURE 8. The result of the third question: By using the proposed Arabic VC tool, do you think this tool might make decryption easy?

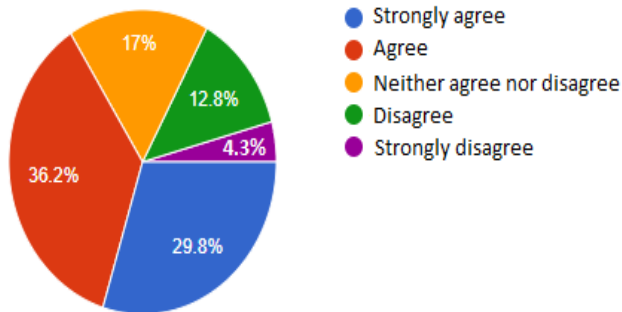


FIGURE 7. The result of the second question: After using the Arabic VC tool, do you think this tool is generally easy to use?

usability of the tool following optimization. Remarkably, despite the fact that well-known words or dictionary-based words can enhance the usability in terms of recognizing the text, some words unfortunately were not recognized correctly due to character confusion.

Although our research focuses on Arabic native speakers, further studies which take the variety of participants in terms of native language into account, may be of interest.

C. SATISFACTION

The results in terms of the three questions are shown in Figures 6, 7, and 8. In particular, Figure 5 shows the results of the first question which indicates that most of the participants were not familiar with the VC technique. It is therefore likely that a connection exists between the usability of applying the VC technique and a lack of familiarity with it. That is, the participants could decrypt the given image using their visual system and recognize the text correctly, though they were not familiar with this technique.

Moreover, Figure 7 shows the result of the second question. In particular, 36.2% and 29.8% of the participants Agreed and Strongly Agreed, respectively, that the tool is generally easy to use. This finding, while preliminary, suggests that the proposed technique is usable with more than 65% satisfaction. Moreover, this finding has important implications for developing such security applications based on developed tool such as Arabic CAPTCHAs.

Furthermore, Figure 8 shows the results with regard to the third question. That is, the response rate was 21.3% at

Strongly Agree, 34% at Agree, 40.4% at Neither agree nor disagree, 4.3% at Disagree and 0% at Strongly Disagree. Generally speaking, the value of the Agree feedback (i.e. 55.3%) which reflects satisfaction, suggests that a strong link may exist between the language of the proposed tool (i.e. Arabic) and its usability. With regard to the neutral feedback (i.e. 40%), the possible interference due to the lack of familiarity with the VC technique cannot be ruled out.

These findings suggest in general that the proposed tool can be utilized in different practical and useful applications, where Arabic is used. For example, potential applications for the proposed tool are its use in electronic voting (e-voting), anti-phishing, Arabic CAPTCHAs and watermarking.

VII. CONCLUSION AND FUTURE WORKS

This paper has given an account of the importance of applying the visual cryptography approach for Arabic texts. In particular, this study was undertaken to develop a tool that encrypts/decrypts images of Arabic texts using the VC approach and to evaluate its usability. This study has shown that the average time required for stacking shares over each other and recognizing the shown text, the effectiveness and the satisfaction were very encouraging. In general, therefore, it seems that the developed tool can be applied in some practical security applications such as Arabic CAPTCHAs. The study has gone some way towards enhancing our understanding of the language effects on usability. The numbers of participants were relatively small, which may be a limitation that needs to be considered. These findings provide the following insights for future research. It would be interesting to investigate the effectiveness of the developed tool with some of the above-mentioned applications. Also, it may be worth enhancing the background and filter out any confusing characters in order for the user to recognize the text correctly.

REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1994, pp. 1–12.
- [2] E. Shahab and H. Abdolrahimpour, "A comprehensive investigation of visual cryptography and its role in secure communications," *PeerJ PrePrints*, vol. 5, no. 1, Jan. 2017, Art. no. e2682.
- [3] M. F. M. Mursi, M. Salama, and M. Mansour, "Visual cryptography schemes: A comprehensive survey," *Int. J. Emerg. Res. Manage. Technol.*, vol. 3, no. 11, pp. 142–154, 2014.

- [4] P. Punithavathi and S. Geetha, "Visual cryptography: A brief survey," *Inf. Secur. J., Global Perspective*, vol. 26, no. 6, pp. 305–317, Nov. 2017.
- [5] H.-C. Lin, C.-N. Yang, C.-S. Lai, and H.-T. Lin, "Natural language letter based visual cryptography scheme," *J. Vis. Commun. Image Represent.*, vol. 24, no. 3, pp. 318–331, 2013.
- [6] S. A. Sattar, S. Haque, M. K. Pathan, and Q. Gee, "Implementation challenges for Nastaliq character recognition," in *Proc. Int. Multi Topic Conf.* Berlin, Germany: Springer, 2008, pp. 279–285.
- [7] R. G. Sharma, "Visual cryptographic techniques for secret image sharing: A review," *Inf. Secur. J., Global Perspective*, vol. 27, nos. 5–6, pp. 241–259, Jan. 2019. doi: [10.1080/19393555.2019.1567872](https://doi.org/10.1080/19393555.2019.1567872).
- [8] J. Nantel and E. Glaser, "The impact of language and culture on perceived website usability," *J. Eng. Technol. Manage.*, vol. 25, nos. 1–2, pp. 112–122, 2008.
- [9] K. Katzner, *The Languages of the World*. Evanston, IL, USA: Routledge, 2002. [Online]. Available: <https://www.questia.com/library/108070247/the-languages-of-the-world>
- [10] J. Ramya and B. Parvathavarthini, "An extensive review on visual cryptography schemes," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol.*, Kanyakumari, India, Jul. 2014, pp. 223–228.
- [11] T. Monoth, "Analysis and design of tamperproof and contrast enhanced secret sharing based on visual cryptography schemes," Ph.D. dissertation, Dept. Computer. Science., Kannur Univ., New Delhi, India, 2013.
- [12] (Feb. 19, 2019). *Digital 2019: Global Internet use Accelerates*. [Online]. Available: <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates>
- [13] H. Kumar and A. Srivastava, "A secret sharing scheme for secure transmission of color images," in *Proc. Int. Conf. Issues Challenges Intell. Comput. Techn. (ICICT)*, Ghaziabad, India, Feb. 2014, pp. 857–860.



SULIMAN A. ALSUHIBANY received the M.Sc. degree in computer security and resilience and the Ph.D. degree in information security from Newcastle University, U.K. He is currently an Associate Professor with the Computer Science Department and also the Head of the Department with Qassim University, Saudi Arabia.

• • •