

A Method to Encode the Fingerprint Minutiae Using QR Code

Mohammed Fadhil Ibrahim
Middle Technical University
Technical College of Management

Abstract

Today, computers and mobiles devices become an essential part that people use to perform a major part of their daily activities. Those devices sometimes become meaningless without being connected to the internet. In addition, people exchange tens of their data cross multiple devices that are connected remotely using internet, the thing that make such data are exposed to be captured. Hence, to overcome such concerns, there is a big necessity to continuously develop new methods to mitigate the threat of data capturing by anonymous people. In this research, we present a method to encode human fingerprint using quick response code (QR Code). The method involves extracting the fingerprint minutiae which depicts the most important features of fingerprint, then that features are turned into image of QR Code format. This method ensures transferring a data with good level of safety since the real data are difficult to be guest. To make the process more complicate, we encrypted the fingerprint features by using (AES) encryption method which make the data meaningless event when they captured by anonymous intruders. After method implementation, the values of PSNR and MSE are calculated to evaluate the performance by comparing the original image with the reconstructed one. The results of the method proved that encoding the fingerprint using QR Codes can be successfully performed and utilized with different applications

Keywords: Biometrics, Fingerprint, QR Code, AES

1. Background

The fast growth of information technology and all related fields is being influencing our life style. Using computer and become a crucial task of our daily activities. In addition, networking, social media, and web-based applications make the information exchanged almost uncovered and prone to be interrupted accidently. Indeed, there are a lot of stories everywhere about hackers and cracker and many attacks are being recorded frequently. This issues are strongly justifies the necessity of information security adoption with many computer related aspects.

One of the most concerns that faces information technology users is sending and receiving documents which mostly in the format of images,

where there are difficulties related with protecting images from being hacked [1]. other techniques used to secure the information throughout hiding them inside other type of media which is known as steganography[2]. This technique helps in protecting the data by masking the most important information to alter it to a hidden manner, so that it is difficult to be observed. On the other hand, cryptography is widely implemented in the context of information security where the data is turned to another format which makes it meaningless unless the decryption is used[3]. Whether cryptography or steganography or both of them is used, it ought to be performed with a convenient level of efficiency and accuracy to satisfy the desired purpose of it [4].

1.1 Fingerprint Biometric

Fingerprint technology is one of the most widely used biometric that has been utilized in order to identify human being. Such technology now used almost everywhere regarding to prove person identity[5]. The minutiae features of the fingerprint are: whorls, loops, arches, and ridges (Figure 1). All these features can be extracted from the image of the fingerprint. Many approaches have been adopted to perform the fingerprint recognition. The main benefit of using fingerprint biometric is low-error rate for such biometric [6, 7].

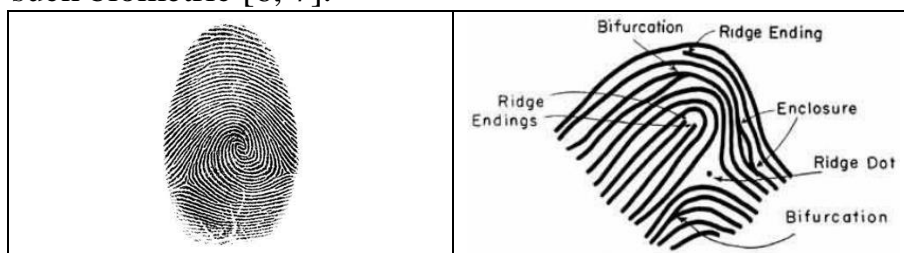


Figure (1): Fingerprint Sample

The uniqueness of a specific fingerprint is identified by a number of features called minutiae [8]. The characteristics of local ridges play a key role in the fingerprint [9]. The ridges formation varies and followed by another one. Officially there are (18) various kinds of fingerprint minutiae that have been recorded by the Federal Bureau of Investigation [10]. Moreover, there are other characteristics such as (islands, short ridges, enclosure, etc.), (Figure 2). Those features are randomly distributed all over the fingerprint. The majority of these features strongly depend on the image quality and capturing efficiency.

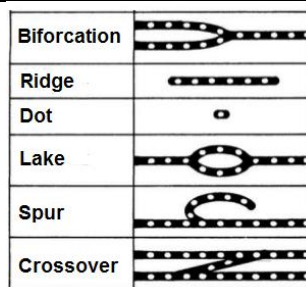


Figure (2): Fingerprint Minutiae

currently, fingerprint minutiae is divided for three specific levels [11], according the image details [12, 13]. The features of (level 1) depict the tiny details of fingerprint image, for instance, deltas and cores (Figure 3). They considered less distinctive features compared with others hence, they are basically employed in terms of classification rather than recognition. The level-2 characteristics are mainly referred to the minutiae, known as the ridge endings and bifurcations (Figure 2). The features of this level considered more distinctive and stable features, thus, they are being utilized with recognition methods due to the reliability and robustness even with low resolution captured images. The features at (level 3) are usually known as the dimensional characteristics of the ridges, ridge contours, and ridge edge features [9]. When implementing all three levels, we can earn the most distinctive features which represent the uniqueness of a particular fingerprint if compared with other one. The thing that makes fingerprint acts as one of the most powerful tool in human recognition context.

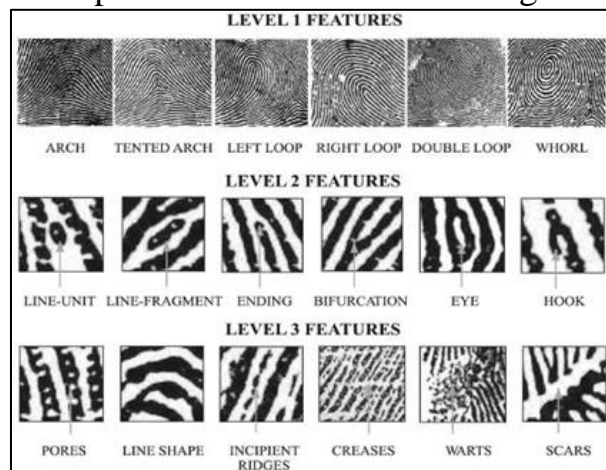


Figure (3): Fingerprint Minutiae Levels [11]

1.2 Cryptography

It is a technique that sends or receives the messages with uncovered method. It is also called the encryption. Its history recorded many encryption attempts that were used in the early ages. The first form of cryptography was registered back to about 1900 B.C by the ancient

Egyptians[14]. Recently, and due to the emerging technology represented by the invasion of computer machine, and telecommunication, no doubt about cryptography and its methods become an essential task has to be taken into consideration especially when dealing with interned connection world. The process of reversing the encrypted text to its original state (plain text) is called decryption[15, 16]. Generally, cryptography is divided into two main approaches which are typically employed to perform different types of cryptography which are:

- Secret/Private Key Cryptography (SKC)
- Public Key Cryptography also known as (PKC).

1.3 Secret Key Cryptography (SKC)

This method employs unique key for encryption and decryption process. Since the same key is involved in this technique, this is why it is known as the symmetric encryption [14]. Here is essential issue, where encryption key must be identified for both of encryption partners, according to this, there is kind of difficulty and risk regarding keys wrongly distributed. Generally, for each network media, there is an intuition inside the people about such environment is considered unsafe. Since the exchanged data are always exposed to be captured. To overcome such problem, the keys are better to be handled in private in a way that being separated from the transmission process itself, or by using another media. There are a number of privileges that clearly extinguish the SKC such as [17]:

- It is faster than other techniques.
- The encrypted data and the decrypted ones can easily being sent in different streams, which enhance the security.
- SKC can attached with other equivalent method to enhance the productivity
- Only the key principals can return the plain information.

According to the mentioned characteristics of SKC, we employed AES algorithm which is one of the most significant encryption algorithms that has been widely involved in the context of information security.

1.4Advanced Encryption Standard (AES)

AES has been created in 1997, and in 2001 it was indorsed by NIST as sophisticated encryption algorithm. AES is falls under the section of the most plausible SKC algorithms. It performs rapidly for the both software and hardware [18]. The procedures of AES have a specific size of blocks within 128 bits, or 256 bits. AES operates at (4*4) matrix. The ciphers of AES are specified through a specific of rounds. Throughout such recurrent rounds, the encryption process is performed perfectly. Each round has

particular procedures and functions involving generating keys and exchanging the data positions. AES also applies a number of reverse rounds to return block the plain text using specified keys.

1.5 Quick Response (QR) Code

QR Code is a two-dimensional symbol. It was founded in 1994 by Japanese Toyota Company, it also endorsed as an ISO international standard (ISO/IEC18004) in 2000. This symbol was basically designed to be used in specific manufacturing controls for parts, after that QR code become widely used in various aspects [19]. Now QR Code can be seen almost everywhere due to the simplicity and efficiency for this code in terms of storing a plausible mount of data with sing image. The QR Code presents a number of characteristics such as:

- The amount of characters that can be stored in QR Code is much more than the data were stored in the prior versions of code which is one dimensional bar code.
- QR code has been presented to be used for free and there are no concerns regarding licences, so that it is available for public use.
- There are no specific requirements for QR Code to be scanned, in facts it is easy to capture it even by using mobile devices. The thing that makes it easy to be implemented for different types of applications.

Therefore, QR Codes have taken intensive popularity all over the world by being adopted in many life aspects [20]. The majority of using these codes in represented by storing URLs, addresses, basic information, and some hidden signs and codes. Generally, the symbol of QR Code image is composed from various areas (patterns) (Figure 4), which can be described as follows [21]:



Figure (4): QR Code Structure [21]

- Pattern-1. Is denoted throughout the large squares dots which are basically locate of the QR Code corners location. Those squares detect the size and positions of the QR Code angles which determines the exact dimensions of it.

- Pattern-2: It depicts the alignment pattern used to fix the distortion of the QR Code. Such distortion appears with capturing the code.
- Pattern-3: the timing pattern, which is embedded with the white and black shapes that arrange alternatively to specify the centre of coordination related to each single cell.
- Pattern-4: Quiet Zone, it is the margin area that ease the QR Code detection process.
- Pattern-5: Data Area, this part formulates the actual data located in the symbol. It also can be consist of particular codes for errors handling procedures.
- The area in the QR code that contains the data (for example a URL) encoded in binary numbers. [22].

QR Codes are more probable to be implemented with such devices due to the ability of capturing theses codes using traditional cameras attached for mobile devices, and eventually extract the desired information[23].

2. Related Work

In this part, we discuss the most significant works that has been presented in the context for using QR Codes in various information technology subject. As we mentioned before; QR Codes exceeds to be using just in production by storing IDs and URLs. Nevertheless, it becomes one of the most emerging techniques that have been widely used in various purposes.

In [24], the authors a new algorithms of reversing data hiding by utilizing QR Codes. The method relies on using QR Code in order to reduce the quantity of information stored in one symbol. The major concern of the study is how to retrieve the original image from the encoded one. After applying the algorithm, the result showed that the method can retain the original picture when the QR Code is captured, the thing that proved the applicability for such implementation of QR Code with images rather than only characters.

In [25], the authors have presented a recognition algorithm based on QR Code. The method tended to overcome the limitations combined with the employment of QR Codes with authentication method. This method achieved whole processes for images to be treated including binarization and normalization. The experiments results proved the method presented a good performance in terms of efficiency and effectiveness when using QR Codes with recognition systems.

There are also other works that dealt with QR Codes in multimedia where the QR Codes can store music and pictures [26], which states a new

way to encode error correction of images on QR Code. Another approach presented by [27], where an animated QR Codes have been presented in addition to embedding a pictures with QR Codes. In [28], a development of image classifier have been presented, the classifier works similar to other face classifiers in order to improve the classification process. Coloured models of QR Codes have been presented in order to increase data rate [29]; Despite colours have the potential to improve appearance and significance. This method has presented robust mechanism for locating encoded data, enhance the colour mapping process.

The aforementioned paragraphs stated a few aspects of using QR Codes in many applications and systems with different perspectives. Therefore we inspired to apply such technique with a new aspect. We propose a method to encode a human fingerprint by using QR Code. This method represents an extension to the previous mentioned work, and proves the usability of QR Codes with different aspect such as images and security

3. Method Implementation and Results Gained

As we mentioned before, our method involves encoding fingerprint image and then hide its information inside a Quick Response Code (QR Code). In our method we use the fingerprint database that have been presented in [30]. The database involves about (4000) images for human fingerprint images with the format of PNG. It has been widely used in several studies that concern with different issues related to fingerprint manipulation. In addition, we encrypt the extracted minutiae using AES algorithm to enrich the method with a level of security. To implement our method we utilized programming tools which are Matlab and Visual C#. The presented method is composed of number of steps (Figure 5). Each step has been performed precisely. The method starts with collecting data, which in our research (Fingerprint images). Each image is turned its corresponding numeric data. As publicly known, each image produces a large amount of data, some of these data are meaningless. Thus, we used a feature extraction method to extract the most significant minutiae and overcome the curse of dimensionality. Then, we have encrypted the features using AES algorithm. After that, we turn the extracted features into QR Code symbol. After implementing the method processes, we reversed the whole process to get the original minutiae. The whole method process worked correctly and the results were good.

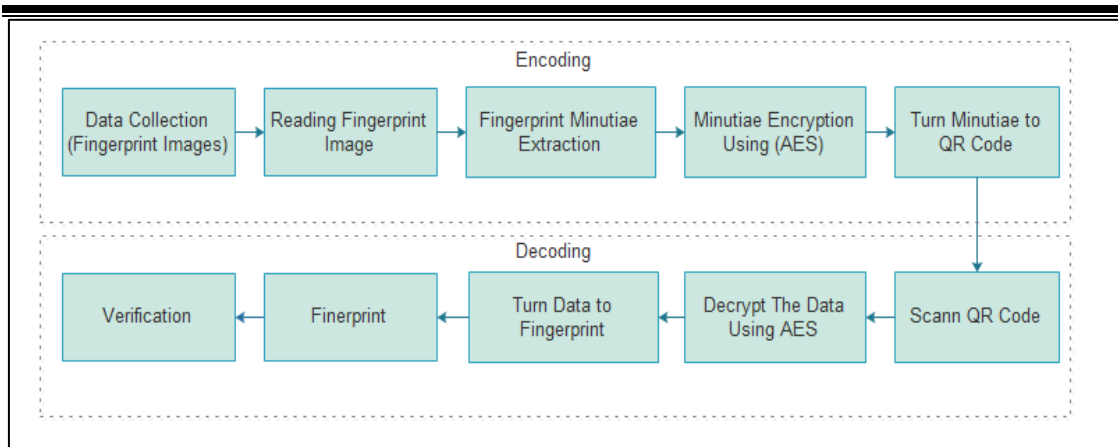


Figure (5): Method Block Diagram

The first step involves the preparation of our dataset; in our experiment we have selected (10) images for fingerprint selected form the above mentioned dataset. Those images represent the experiment input. First we read images data by transferring each image to its corresponding numerical data, then, the image is turned to a grayscale state since in fingerprint the colors are meaningless and causes noisy date.

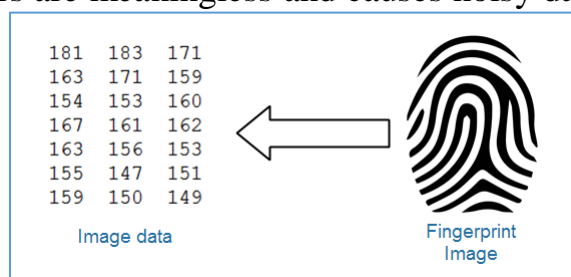

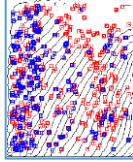
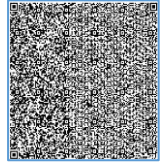

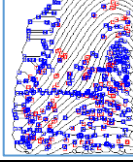
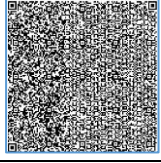

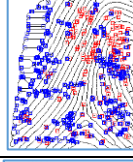
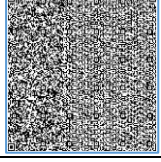

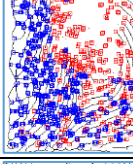
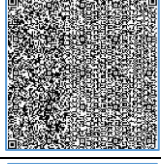

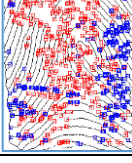
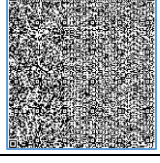


Figure (6): Reading Fingerprint Image

After that the minutiae of the input fingerprint is founded. This step insures the use of only the most significant data out of all data inside fingerprint image. Then the finger minutiae has been encrypted using AES algorithm to enhance the security side in case using such fingerprint across networks which might be under unknown threats. Finally, the encrypted data has been turned into QR Code which can be scanned using QR Code reader. Note that even the data is captured by using any QR Code scanner or even standard camera; the captured data still meaningless due to the encryption and this is the main idea behind using data encryption method (Table 1).

Table (1): Illustration of the Method Implementation and Outputs

Seq	Fingerprint Image	Minutiae	QR Code
1.			
2.			
3.			
4.			
5.			

As generally known, for every method, there should be a verification process in order to ensure the usability and efficiency of any presented method. Hence we verified our method by calculating the Peak Signal-to-Noise Ratio (PSNR), which measures the quality of images recreation by comparing the original image with the reconstructed one. In or case we compared the initial image and the new one after scan it and decrypt the data inside it. The values of PSNR can be seen in (Table 2). In addition, we also calculated the value if Mean Square Error (MSE) for each fingerprint image to measure the difference between the original image and the reconstructed one. All results are displayed in (Table 2).

Table (2): The Values of PSNR and MSE for the Processed Images

Processes*	MSE	PSNR
1.	3.18	39.87
2.	4.55	41.58
3.	3.16	43.16
4.	2.73	43.79
5.	3.92	42.22
6.	2.75	43.77
7.	0.91	48.57
8.	0.23	45.57
9.	3.14	42.64
10.	3.62	42.58

4. Discussion

According to the values of PSNR; it can be clearly seen that the method is worked fine and it reaches the purpose of making it. Regarding to mathematical principals, the value of PSNR is represented by the formula $(2^{\text{Bits}} - 1)$ [31], nevertheless the images we work with are from depth of (8 Bits/Pixel), that means the maximum PSNR value should not be more than (255) . Refer to (Table 2 and Figure 7) we can see that the maximum value of PSNR is (48.57), which means the results falls under the acceptable range. On the other hand, the maximum value of MSE is (4.55), and since, all MSE values are small then our results are goon according to the concept of MSE, where the smaller value gives the better results [31].

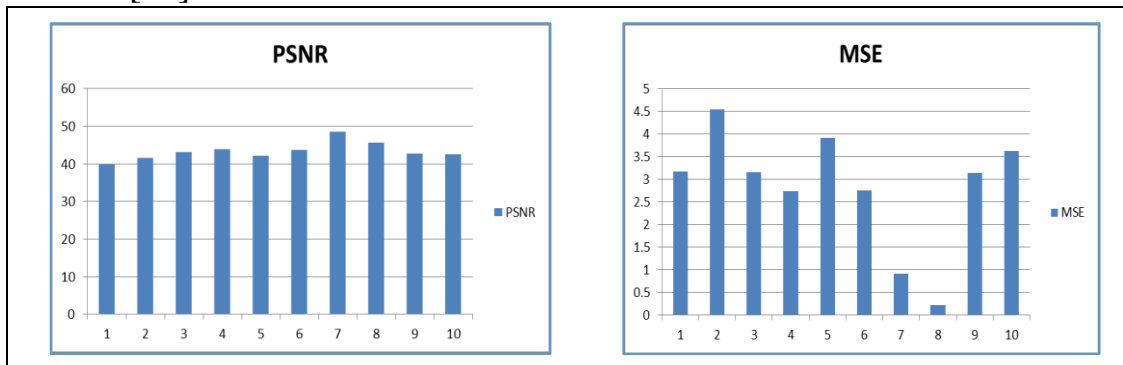


Figure (7): The Bar Chart of PSNR and MSE

5. Conclusion and Future Trends

After implementing our method, there are a number of conclusions have been formulated which are:

* : Refers to the whole process of comparing the original image with the reconstructed one

1. QR Codes can be implemented with more sophisticated computer relate aspects rather that storing URLs.
2. Fingerprint can be encoded successfully using QR Code. Which might utilized in data hiding methods.
3. According to the values of PSNR and MSE, our method has been implemented successfully.

For future trends, this method can be implemented with different type of biometric such as face, iris, retina, and so on. In addition, enhance the method to work with mobile devices with different platforms.

References

- [1] D. Bissessar, C. Adams, and A. Stoianov, "Privacy, Security and Convenience: Biometric Encryption for Smartphone-Based Electronic Travel Documents," in *Recent Advances in Computational Intelligence in Defense and Security*, ed: Springer, 2016, pp. 339-366.
- [2] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*: CRC Press, 2017.
- [3] J. Katz and Y. Lindell, *Introduction to modern cryptography*: CRC press, 2014.
- [4] M. Rawde, M. Kumbhare, S. Chaudhari, S. Bhongade, and V. Bhagat, "Novel Approach towards Higher Security Using Crypto-Stego Technology," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 4, 2015.
- [5] M. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications*, vol. 42, pp. 8198-8211, 2015.
- [6] D. Bhattacharyya, R. Ranjan, A. Farkhod Alisherov, and M. Choi, "Biometric authentication: A review," *International Journal of u-and e-Service, Science and Technology*, vol. 2, pp. 13-28, 2009.
- [7] M.-C. Cheung, M.-W. Mak, and S.-Y. Kung, "Intramodal and intermodal fusion for audio-visual biometric authentication," in *Intelligent Multimedia, Video and Speech Processing, 2004. Proceedings of 2004 International Symposium on*, 2004, pp. 25-28.
- [8] D. Peralta, M. Galar, I. Triguero, D. Paternain, S. García, E. Barrenechea, *et al.*, "A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation," *Information Sciences*, vol. 315, pp. 67-87, 2015.
- [9] N. Zaeri, "Minutiae-based fingerprint extraction and recognition," in *Biometrics*, ed: InTech, 2011.
- [10] R. Mueller, "Federal Bureau of Investigation," ed, 2008.
- [11] M. Dubey and S. Sahu, "Fingerprint Minutiae Extraction and Orientation Detection using ROI (Region of interest) for fingerprint matching," *International Journal of Scientific & Engineering Research*, vol. 5, pp. 289-300, 2014.
- [12] P. Zhang, C. Li, and J. Hu, "A pitfall in fingerprint features extraction," in *Control Automation Robotics & Vision (ICARCV), 2010 11th International Conference on*, 2010, pp. 13-18.
- [13] J. Feng, Z. Ouyang, and A. Cai, "Fingerprint matching using ridges," *Pattern Recognition*, vol. 39, pp. 2131-2140, 2006.
- [14] G. C. Kessler, "An overview of cryptography," ed: Gary C. Kessler, 2003.
- [15] D. E. Robling Denning, *Cryptography and data security*: Addison-Wesley Longman Publishing Co., Inc., 1982.

A Method to Encode the Fingerprint Minutiae Using QR Code

Mohammed Fadhil Ibrahim

- [16] W. Stallings and M. P. Tahiliani, *Cryptography and network security: principles and practice* vol. 6: Pearson London, 2014.
- [17] P. Gaži and S. Tessaro, "Secret-key cryptography from ideal primitives: A systematic overview," in *Information Theory Workshop (ITW), 2015 IEEE*, 2015, pp. 1-5.
- [18] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, *et al.*, "The Twofish Team's Final Comments on AES Selection," *AES round*, vol. 2, 2000.
- [19] T. J. Soon, "QR code," *Synthesis Journal*, vol. 2008, pp. 59-78, 2008.
- [20] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, *et al.*, "QR code security," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010, pp. 430-435.
- [21] I. Jelić and D. Vrkić, "QR codes in library-Does anyone use them?," in *Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on*, 2013, pp. 695-699.
- [22] R. Ashford, "QR codes and academic libraries: Reaching mobile users," *College & Research Libraries News*, vol. 71, pp. 526-530, 2010.
- [23] Y.-P. Huang, Y.-T. Chang, and F. E. Sandnes, "Ubiquitous information transfer across different platforms by QR codes," *Journal of Mobile Multimedia*, vol. 6, pp. 3-13, 2010.
- [24] H.-C. Huang, F.-C. Chang, and W.-C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," *IEEE Transactions on Consumer Electronics*, vol. 57, 2011.
- [25] Y. Gu and W. Zhang, "QR code recognition based on image processing," in *Information Science and Technology (ICIST), 2011 International Conference on*, 2011, pp. 733-736.
- [26] K. Fujita, M. Kuribayashi, and M. Morii, "A study of image displayable design qr code," *IEICE Technical Report*, pp. 39-44, 2011.
- [27] S. Ono, K. Morinaga, and S. Nakayama, "Animated two-dimensional barcode generation using optimization algorithms," in *SCIS & ISIS SCIS & ISIS 2008*, 2008, pp. 1232-1237.
- [28] L. Belussi and N. Hirata, "Fast QR code detection in arbitrarily acquired images," in *Graphics, Patterns and Images (Sibgrapi), 2011 24th SIBGRAPI Conference on*, 2011, pp. 281-288.
- [29] D. Parikh and G. Jancke, "Localization and segmentation of a 2D high capacity color barcode," in *Applications of Computer Vision, 2008. WACV 2008. IEEE Workshop on*, 2008, pp. 1-6.
- [30] C. Watson and P. Flanagan, "NIST Special Database 14 Mated Fingerprint Card Pairs 2 WSQ Compressed Images," 2016.
- [31] D. Salomon, *Data compression: the complete reference*: Springer Science & Business Media, 2004.

المستخلص:

تشكل الحواسيب والاجهزة المحمولة اداة مهمة يستخدمها الناس لاداء مختلف الفعاليات اليومية، وفي كثير من الاحيان تكون هذه الاجهزة عديمة الفائدة في حالة انعدام توصيلها بشبكة الانترنت. فضلا عن ذلك، يتبادل الناس يوميا كمًا هائلًا من البيانات والمعلومات باستخدام الاجهزة الموصولة بالانترنت، مما يجعل هذه البيانات والمعلومات عرضة للاختراق. وبغية التغلب على هذه المخاوف، يتزايد عدد التقنيات والطرق المستخدمة في حماية البيانات المنقولة بواسطة الانترنت. في بحثنا هذا نقدم طريقة لترميز بيانات بصمة الابهام وتحويلها الى رمز سريع الاستجابة (QR Code). يتم بموجب هذه الطريقة استخلاص الخصائص المعنوية لصورة البصمة وتحويلها الى رمز سريع الاستجابة. ولاضفاء حماية للبيانات، تم الاعتماد على خوارزمية التشفير (AES)، بغية تشفير الخصائص المستخلصة قبل تحويلها الى رمز. هذا الاجراء يجعل من البيانات عديمة الفائدة في حالة التقاطها نظرا لتشفيرها. وللتحقق من تطبيق الطريقة تم احتساب مقدار نسبة التشوه (PSNR) ومجموع مربعات الخطأ (MSE) والتي تقيس نسبة التغيير الحاصل في الصورة الجديدة مقارنة بالصورة الاصلية. اثبتت النتائج المستحصلة انه يمكن ترميز صورة بصمة الابهام وتحويلها الى رمز سريع الاستجابة والعكس بالعكس بنجاح. ان تطبيق هذه الطريقة يفتح الابواب امام توظيف رمز سريع الاجابة مع بيانات بايومترية اخرى.