Scientific Journal for Damietta Faculty of Science **12**(1) 2022, 39-49
DOI: 10.21608/SJDFS.2018.194790
ISSN Print 2314-8594
ISSN Online 2314-8616

https://sjdfs.journals.ekb.eg/

Information Hiding Using Coverless Steganography System Based on Image Generation

Al-Hussien Seddik[1], Mohammed Salah[*2], Gamal Behery[2] and Ahmed El-Harby[2]

[1]Department of computer science, Faculty of Science, Minia University, Minia, Egypt.
[2]Department of computer science, Faculty of Computers and Artificial Intelligence, Damietta University, New Damietta, Damietta, Egypt

Received: 23 October 2022 /Accepted: 25 October 2022

[*] Corresponding author's E-mail: msr_cs_87@du.edu.eg

Abstract

Image generation plays an important role for designing a robust coverless steganography system able to face different information hiding challenges. This paper proposes an image generation- based coverless steganography system which has the capability to transmit the secret message safely. The generated image is similar to the famous Quick Response (QR) code image; it is called semi-QR code in that paper. The proposed system consists of two processes, the first process, secret message hiding process, is used at the sender of the message and is responsible for generating the semi-QR code image from only the secret message bits using the hiding algorithm. While the second process, secret message extraction process, is used by the receiver of the message who can retrieve the secret message from the received semi-QR code image using the extraction algorithm. Finally, a coverless steganography system that implements the proposed algorithms has been built. To evaluate the effectiveness of these algorithms, experiments have been carried out using different evaluation measures, namely the Bit Error Rate (BER) and Success Rate (SR). The results confirmed that the proposed system is better than other traditional steganography systems achieving higher capacity and a higher level of robustness than them.

Keywords: coverless steganography; information hiding; information security; QR code.

Introduction

Nowadays, transmission of sensitive data over any communication channel are considered primary challenge. These sensitive data may be attacked through illegal actions [1]. Cybercrimes and cyberattacks [2] are two important terminologies in securing the transmission process for the internet as a public channel [3]. Many methodologies are used to secure data such as steganography.

Steganography is a technique used to hide an information in any other type of another information without changing the second information to appear as an original one [4]. Some researchers define steganography as "hiding in plain sight" which means that the sent message is out of the open for all to see as due

to its secret existence. Some forms of steganography are done with unnoticed way from the sender to the recipient of the message [5].

Generally, steganography as a system consists of two components, the first one called embedding which is responsible for concealing the secret message within a cover file. The second component is called extraction which retrieves the hidden secret message from the sent stego file, the cover file after hiding the message in it [6].

In 2014, a group of researchers discussed an idea to hide data without using a cover file. This terminology is called coverless steganography. Coverless steganography can be executed by a cover generation using the secret message bits themselves, this generated cover implies the secret message and it may be an image, video, audio, or text file. The other form of coverless steganography is building an image database consists of a number of natural images, then these images are divided into sub-blocks. Finally, the secret message bits are compared with these images sub-blocks to match between them [6].

Yun Tan et al. [7] used motion analysis of video to develop a coverless steganography technique. Robust histograms of oriented optical flow (RHOOF) were generated for all videos found in the database and the database was indexed. These indices and RHOOF hash sequences are transmitted to the recipient of the message as a mapping. The RHOOF hash sequences were computed from the sent video which helped in retrieving the secret message. All videos which were used as a covers do not lose any of their contents through processes of transmitting and receiving.

Al-Hussien et al. [8] generated a jigsaw puzzle image with the aid of the cover image to build a new coverless image steganography technique. This approach used a natural image as a cover image, then split it into a similar sub-blocks row by row then column by column. Zeros and ones of the secret message bitstream were represented by blanks and tabs for each puzzle piece, respectively. The recipient received the created jigsaw puzzle image as a stego image in which he/she had the ability to retrieve the message from the stego image using the secret message retrieval algorithm.

The main contribution of this paper is to design a robust coverless image steganography system based on image generation in the form of semi-QR code image driven from only the secret message. The generated system is able to secure data during the transmission process through any digital communication channel, this system has the ability to not lie on the trap of the attackers.

The paper is arranged as follows: Section 2 describes the proposed method in details. Section 3 introduces the performance evaluation metric. Section 4 deducts the experimental results. Finally, section 5 summaries the conclusion of the paper.

The Proposed System

The main purpose of the proposed system is to build a robust system able to hide a huge amount of data in a secured form before transmitting them to the receiver. The system consists of two main components, each terminal (i.e, sender and receiver) has one component. At the first terminal, the secret message bits are transformed into the form of semi-QR code image using the hiding algorithm. This image is considered the stego image which sent to the other terminal. At the second terminal, the semi-QR code image is used as an input to the extraction algorithm which retrieves the secret message from this semi-QR code image. The structure of the proposed system is illustrated in figure 1.

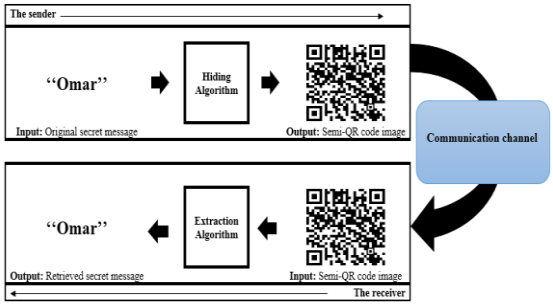

Figure 1. The structure of the proposed system

The following subsection introduces an overview of a QR code which is used in hiding the secret message into the form of semi-QR code image.

QR Code

A QR code (an abbreviation for Quick Response code) is a type of two-dimensional matrix barcode [9,10]. This code was invented by Denso Wave,

Japanese automotive company, in 1994 [11,12]. A barcode is a machine-readable optical label that can store data about an item. On the other hand, QR codes can attach any data types. In practice, QR codes often contain data for a location, identifier, tracker that points to a website or application, or information for a map. A QR code uses many standardized encoding modes (numeric, alphanumeric, byte/binary) to store data efficiently; extensions may also be used [13]. Recently, QR codes are used for other different purposes outside industry as they have many properties such as fast readability and high storage capacity compared with classical traditional barcodes. Some applications of a QR codes include product tracking, item identification, time tracking, document management, and general marketing [14].

The architecture of QR code consists of black squares arranged together in a square grid on a white background, these squares can be read by any QR reader such as a mobile camera or a scanner. Reed–Solomon error correction is used to proceed the image interpretation process. Finally, The required data is then extracted from patterns that are present in both horizontal and vertical components of the image [14].

The following subsections 2.2 and 2.3 describe the two processes of the system in details, hiding process and extraction process, respectively.

The Hiding Process

In this process, the secret message bits are fed to the system which generates the semi-QR code image. This image is considered the stego image which sent to the receiver. The following sub-sub-section describes the hiding algorithm in details, see figure 2 which illustrates the main phases of secret message hiding process.

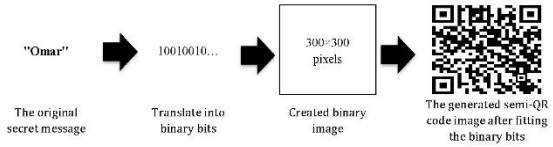

Figure 2. The main phases of secret message hiding process.

Secret Message Hiding Algorithm

The hiding algorithm works as follows, see algorithm 1. Firstly, the secret message is converted into a sequence of binary bit-streams (i.e, ones and zeros). Then, a binary image is created and set its pixels to white. After that, the converted binary bit-streams are represented in this created binary image based on the value of the current bit (if the current bit is zero, set the current image pixel value to black; else if the current bit is one, let the current pixel as it is, white pixel). This step is repeated until representing all bits of the original secret message. The bits of the secret message are represented in whole image except the four regions of the alignment patterns (top left, top right, bottom left, and bottom right). Also, the represented pixel size (RPS) and alignment patterns size (APS) are defined in equations 1 and 2, respectively.

Algorithm 1 Secret Message Hiding

START
INPUT: The original secret message (OSM).
OUTPUT: Semi-QR code image (SQRI).
1: Create a binary image and set its pixels to white.
2: Determine the represented pixel size, RPS, according to the secret message length from equation (1).
3: Determine the size of the alignment patterns, APS, of the semi-QR code image from equation (2).
4: Convert OSM into binary bit-streams.
5: Add supplementary virtual bits to OSM bits, as shown in equation (3), if the actual length of the OSM is less than any length mention in equation (1).
6: **For** all bits of OSM **do**
7: **If** the target bit (The bit needed to be represented) == 0, **then**, set the current image pixel to zero, black pixel.
8: **Else if** the target bit == 1, **then**, let the current image pixel as it is, white pixel.
9: Repeat steps 7 and 8 until all bits of the OSM are represented.
10: **End if**
11: **End for**
12: Return the generated semi-QR code image (SQRI).
END

The structure of the generated semi-QR code image is illustrated in figure 3 and it consists of two main zones. The first zone is called the alignment patterns zone which contains four regions (top left, top right, bottom left, and bottom right). Whereas the second zone is called data representation zone which can hold the secret message bits as shown below:

Figure 3: Layout of the generated QR code image.

Equation 1 calculates RPS needed to fit into the semi-QR code image. RPS is determined

according to the length of OSM, L; the created binary image is square image with a dimension of 300 pixels for each width and height. RPS is calculated as follows:

$$RPS = \begin{cases} H * 0.03 + 1 & .if \ \min = 0 < L \leq \max = 728 \\ H * 0.02 & .if \ \min = 728 < L \leq \max = 2328 \\ H * 0.02 - 1 & .if \ \min = 2328 < L \leq \max = 3432 \\ H * 0.02 * \frac{2}{3} & .if \ \min = 3432 < L \leq \max = 5456 \\ H * 0.01 & .if \ \min = 5456 < L \leq \max = 9832 \\ H * \frac{0.02}{3} & .if \ \min = 9832 < L \leq \max = 22328 \end{cases} \quad (1)$$

where H is the height of the created binary image in pixels and L is the OSM length in bits. Also, equation 2 determines the size of the four alignment patterns. The size of the first three alignment patterns are identical but the fourth alignment pattern has smaller size than them. APS is calculated as follows:

$$APS = \begin{cases} RPS * 6 & . \text{ for the first three alignment patterns} \\ RPS * 5 & . \text{ for the fourth alignment pattern.} \\ & \text{bottom right pattern} \end{cases} \quad (2)$$

where RPS is a square matrix of size RPS*RPS and its value is calculated as shown above in equation (1).

The general working mechanism of data representation in the semi-QR code image as follows: If the actual length of OSM is in between the minimum and maximum lengths mentioned in equation (1), then virtual bits are added to complete the final length which is represented in the generated semi-QR code image. Also, a separator is used to separate between the actual bits of OSM and supplementary virtual bits. The final represented bits (FRB) is calculated as shown in equation 3:

$$FRB = AB + S + VB \quad (3)$$

where AB, S, and VB represent the actual bits of OSM, a separator and its value equals to eight consequent ones which is considered an indicator for the end of the actual bits, and a set of random supplementary virtual bits with a random size, respectively. Finally, the length of FRB is the maximum length as written in equation 1. Figure 4 illustrates a samples of semi-QR code images generated by the system with different represented pixel sizes and data lengths.

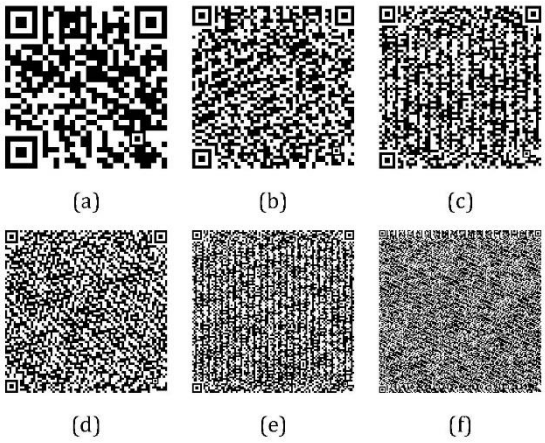

Figure 4. Samples of the generated semi-QR codes with different lengths and pixels sizes. (a): RPS = 10 pixels and L = 728 bits, (b): RPS = 6 and L = 2328, (c): RPS = 5 and L = 3432, (d): RPS = 4 and L = 5456, (e): RPS = 3 and L = 9832, and (f): RPS = 2 and L = 22328**.**

The Extraction Process

In this process, the receiver uses the secret message extraction algorithm to retrieve OSM from semi-QR code image which is delivered from the sender. Sub-section 2.3.1 describes the extraction algorithm in details and the phases of secret message extraction are illustrated in figure 5.

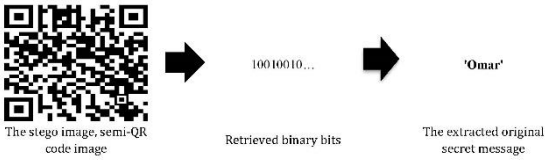

Figure 5. Main phases of secret message extraction process.

Secret Message Extraction Algorithm

This algorithm is responsible for retrieving OSM from semi-QR code image obtained from the sender terminal. The extraction algorithm, see algorithm 2, works as follows: Firstly, the system scans the inserted binary semi-QR code image to calculate the size of the four alignment patterns, APS. Then, determine the represented pixel size, RPS, to locate the pixel's representation zone. After that, all pixels of the pixel's representation zone are checked; if this pixel is black (i.e, its value equals to zero), return the bit 0; else if this pixel is white (i.e, its value equals to one), return the bit 1. Repeat this step until whole image pixels are scanned and then collect each 8-bits together translating them into characters. Finally, concatenate these

characters and return the original secret message, OSM.

Algorithm 2 Secret Message Extraction

START
INPUT: Semi-QR code image (SQRI).
OUTPUT: The original secret message (OSM).
1: Scan the black/white semi-QR code image to calculate the alignment patterns size, APS.
2: Calculate the represented pixel size, RPS, from the value of APS.
3: Initialize the original secret message variable (OSM) with null.
4: **For** all pixels of semi-QR code image **do**
5: **If** the pixel value == 0, **then**
6: Concatenate the bit '0' to the variable OSM.
7: **Else if** the pixel value == 1, **then**
8: Concatenate the bit '1' to the variable OSM.
9: **End if**.
10: **End for**.
11: Segment OSM into chunks of bytes and translate them into characters.
12: Collect all translated characters.
13: Return the original secret message (OSM).
END

Performance Evaluation Measurements

A coverless steganography system, which implements the two proposed algorithms, shown in figures 3 and 7, has been designed. Two evaluation metrics, namely bit error rate and success rate, are used to measure the system performance with different represented pixels size and secret message lengths. These metrics are defined in the following two sub—sections 3.1 and 3.2 as follow:

Bit Error Rate (BER)

BER measures the difference between the original secret message bits and the extracted bits from the semi-QR code image as a stego image. BER works by applying XOR operation between bits of the original secret message and bits of the retrieved message. It is given by [15]:

$$\mathbf{BER} = {}^{E}/_{L},\ \mathrm{E} = \sum_{i=1}^{L} Xi \oplus Yi \qquad (4)$$

where E, L, X, and Y are the number of invalid bits of the retrieved message, the total length of the original secret message, the bits of the original secret message, and bits of the retrieved message, respectively. The system accuracy is determined based on the value of E. If E equals to zero, this indicates that there are no errors found (i.e, the bits of the retrieved message and the bits of the original secret message are identical) and the system achieves 100% as a success rate. Else if E is greater than zero, this is an indication that the bits of the retrieved message had been altered or damaged during the extraction process and the system does not achieve 100% as a success rate.

Success Rate (SR)

SR calculation depends on the value of BER. It measures the ratio of percentage for the retrieved message bits, SR is given by:

$$\mathbf{SR} = 100\ \% - \mathrm{BER}\ (\%) \qquad (5)$$

where the value of BER is defined above in equation 4. The relation between the value of SR and BER is reverse relation (i.e, the higher the BER value, the lower SR value and vice versa). If the value of SR equals to 100 %, this indicates that the retrieved message is correctly retrieved with no modified or damaged bits during the extraction process. Contrarily, if SR < 100 %, this is an indication that there are altered bits changed by the attackers.

Experiments and Results

This section describes the experiments that have been conducted to study the performance of the proposed coverless steganography system compared with other systems and to check the ability of the system to represent a maximum amount of data in a secure form. MATLAB was used for conducting the results [3,16,17].

The Designed Information Hiding Coverless Steganography System

As mentioned above, the proposed system consists of two main algorithms, hiding algorithm and extraction algorithm. Figure 6 shows the interface of the implemented hiding algorithm of the system. Also, the interface of the implemented extraction algorithm of the system is illustrated as shown in figure 7.

Figure 6. (a): The main interface for the proposed coverless steganography system, (b): The main interface 229 for hiding process (generating semi-QR code image), and (c): Secret message hiding algorithm statistics.

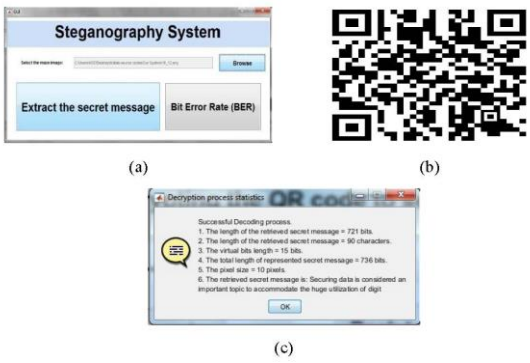

Figure 7. (a): The main interface for extraction process, (b): The inserted semi-QR code image, and (c): The extracted secret message and its statistics.

The Hiding Capacity

One of the main goals of any coverless steganography system is how to increase the hiding capacity. So the hiding capacity is considered an important criterion to evaluate the steganography system accuracy. Hiding capacity is defined as the amount of data that the system can hide successfully [18]. Table 1 presents the hiding capacity of the proposed system compared with other systems.

Table 1. The hiding capacity.

Method	Hiding Capacity (in bits)
S. Li et al. [19]	8
Y. Cao et al. [20]	14
S. A. Baker et al. [4]	1 ~ 15
Z. L. Zhou et al. [21]	16
S. Zheng et al. [17]	18
Y. Tan et al. [7]	32
Y. Cao et al. [22]	36
Y. Cao et al. [23]	68
L. Zou et al. [24]	80
Z. Zhou et al. [16]	384
A. H. S. Saad et al. [8]	760
Y. Luo et al. [25]	800
The proposed system	2328

The previous table showed the improvement of hiding capacity of the proposed system which was the largest one among all capacities of almost all other coverless steganography systems, which is 2328 bits. Table 2 compares the proposed system with other systems in the term of the number of images required to hide different data sizes. Figure 8 shows a comparison between the proposed system and other systems in the term of hiding capacity in bits.

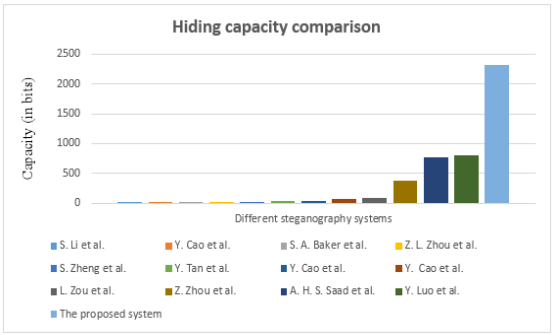

Figure 8. Hiding capacity comparison.

Table 2. The number of generated images required to hide different data sizes.

Data sizes	Z. Zhou et al. [26]	X. Zhang et al. [3]	S. Zheng et al. [17]	Y. Tan et al. [7]	A. H. S. Saad et al. [8]	The proposed system
1 byte	1	2~9	2	1	1	1
10 bytes	10	7~81	6	3	1	1
100 bytes	100	55~801	46	25	1.05	1
1 kilobyte	1024	548~8193	457	256	10.7	3.4

The previous table showed that the proposed system generates the minimum number of images compared with other systems. Only one image is required to hide 1 byte, 10 bytes, and 100 bytes of data and roughly 4 images for hiding 1 kilobyte of data. Figure 9 illustrates a comparison between the proposed system and other systems in the term of number of required images needed to hide different data sizes.

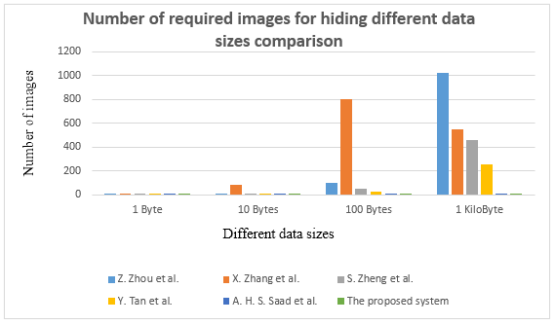

Figure 9. Comparison in the term of number of required images needed to hide different data sizes.

Robustness

Resisting any coverless system against any attacks can be defined as the robustness. The robust degree depends on the value of SR. The closer the value of SR to 100%, the higher robustness degree of the system. Sub-sub-sections 4.3.1, 4.3.2, and 4.3.3 test the proposed system using image scaling attack, JPEG Image Compression Attack, and Adding Noise Attack, respectively.

Image Scaling Attack

Image scaling plays an effective role and is considered an important criterion as an attack. It has the ability to alter the represented bits inside the semi-QR code image [27] during extracting them from the stego image at the receiver terminal. SR values are determined at different image scaling ratios vary from 0.3 to 3, as shown in table 3. The actual size of the image is at scaling ratio 1. If the image scale ratio is less than 1, this means that the image content dimension will be decreased; else if the image scale ratio is greater than 1, this indicates that the image content dimension will be increased.

Table 3. SR values for image scaling attack.

System	Image scaling ratios					
	0.3	**0.5**	**0.75**	**1.5**	**2**	**3**
X. Zhang et al. [3]	85.4 %	94.3 %	96.1 %	98.4 %	-	-
J. Wu et al. [15]	98.5 %	99.1 %	99.8 %	97.5 %	-	-
The proposed system	Failed	100 %	100 %	100 %	100 %	100 %

The results in table 3 confirmed that the system has the best SR value with 100 for all tested scaling ratios except at ratio 0.3 and this indicates that the secret message was extracted correctly with no altered or damaged bits. There is an exception for scaling ratio 0.3, the system fails to extract the secret message correctly with no errors due to the distortion occurred in identifying the represented pixels of semi-QR code image. Figure 10 shows a comparison between the proposed system and other systems for testing the image scaling attack.

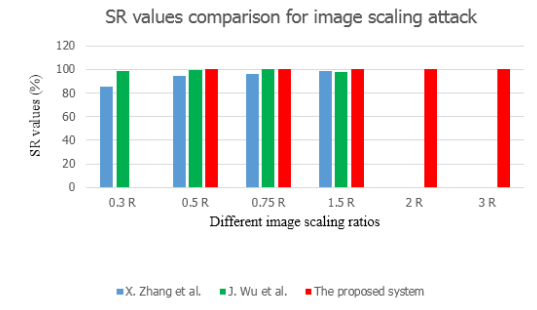

Figure 10. Image scaling attack comparison

JPEG Image Compression Attack

Some transmission communication channels such as Facebook, WhatsApp, and yahoo change the sent images content by compressing them [28]. This compression may effect on the transmitted images and damage the data in which this image represents. JPEG image compression was applied at different image qualities, 90%, 80%, 70%, 60%, and 50%. Table 4 compares the SR value of the proposed system with other systems. The format of original generated semi-QR code image was .PNG and its size was140 KB. While the sizes of the compressed image files were 91 KB, 77 KB, 53 KB, 30 KB, and 26 KB correspond to the image qualities mentioned above, respectively.

Table 4. SR values for JPEG image compression attack.

System	Image qualities				
	90%	**80%**	**70%**	**60%**	**50%**
X. Zhang et al. [3]	97.8 %	-	96.2 %	-	84.9 %
S. Zheng et al. [17]	100%	-	92 %	-	-
J. Wu et al. [15]	100%	-	99.8 %	-	99.3 %
The proposed system	100%	100%	100%	100%	100%

The results of table 4 showed that the proposed system is the best one achieving 100 % as a success rate for all image qualities, this is an indication that the system could deal with and resist against the JPEG image compression attack and the secret message was correctly extracted with no lost or damaged bits. Figure 11 shows a comparison between the proposed system and other systems in the term of JPEG image compression attack.

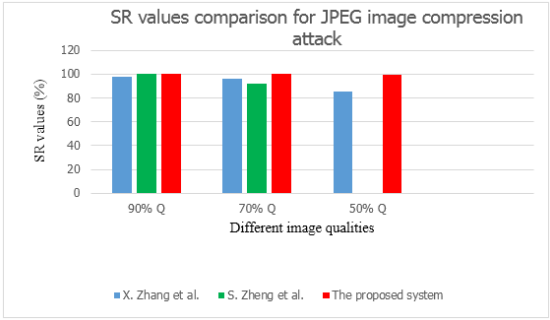

Figure 11. JPEG image compression attack comparison.

Adding Noise Attack

The image quality may be affected as a result of adding an arbitrary noise in the form of random pixels, this noise can threat the image as it may distort the image features. Salt and pepper noise is one of the noise types, it can add a set of random dots which may flip the value of the pixels in a binary image (i.e, a black pixel is flipped to white pixel and vice versa). Noise density is defined as the number of added black/white pixels to the image. The larger the noise density, the larger the image distortion and the smaller the image quality. It's easily for the human eyes to detect the added black/white dots specially with the high noise density values. The proposed system implements salt & pepper noise attack [29] using various densities vary from 0.01 to 0.09 as shown in table 5.

Table 5. SR values for adding "salt & pepper" noise attack.

System	Noise densities								
	0.01	**0.02**	**0.03**	**0.04**	**0.05**	**0.06**	**0.07**	**0.08**	**0.09**
Y. Cao et al. [23]	98%	94%	89%	84%	-	-	-	-	-
Z. L. Zhou et al. [21]	99%	96%	95%	91%	-	-	-	-	-
J. Wu et al. [15]	100%	100%	100%	99.95%	-	-	-	-	-
The proposed system	100%	100%	100%	100%	100%	100%	100%	100%	100%

As shown above, the results showed that the proposed system is the best one among all compared systems achieving 100% success rate for all used noise densities. This means that after adding salt & pepper noise, the system was able to extract the secret message from the semi-QR code image correctly with zero BER value. Finally, salt and pepper noise attack, using different densities, does not threat the system achieving accuracy 100 %.

Other Different Attacks

Different communication channels [30], color space conversion, and Image format conversion play a necessary role as an attacker that test the durability of the proposed system against these attackers. Facebook, WhatsApp, and yahoo are communication channels that may compress the image and change its quality during transmitting the messages from the sender to the receiver. The proposed system extracted the secret message correctly after sending, receiving, and sending back it. Color space such as binary and grayscale image may also change the content of the image, this may reflect unsuccessful secret message extraction process. Table 6 summarizes these attacks and the reaction of the proposed system.

As shown above, the proposed system resists to all threats with accuracy 100 % as a success rate. This is an indication that the system can secure the retrieved message with no damaged or lost bits.

Table 6. SR values for many different attacks.

Different attacks		**The proposed system**
Facebook communication channel attack	Sending & receiving	100 %
WhatsApp communication channel attack	Sending & receiving	100 %
Yahoo communication channel attack	Sending & receiving	100 %
Color space conversion	Binary	100 %
	Grayscale	100 %
Image format conversion (PNG)	BMP (24 bits)	100 %
	JPG	100 %
	TIFF (32 bits)	100 %
	GIF (8 bits)	100 %
	256 color bitmap (8 bits)	100 %

Conclusion and Future work

This paper proposes an effectiveness coverless steganography system for information hiding based on image generation, this image is semi-QR code image. The system works as follows: at the sender terminal, the original secret message is fed to the system generating semi-QR code image using the secret message hiding algorithm. This generated image is considered the stego image sent to the receiver. On the other hand, the receiver inserts the received semi-QR code image, then the secret message is retrieved from that image using the secret message extraction algorithm. The

experimental results and analysis in subsection 4.2 demonstrated that the system achieved a high hiding capacity which is 2328 bits, as shown in tables 1 and 2. Also, the system has a high level of robustness for almost attacks which achieved 100% as a success rate, as shown in subsection 4.3 and tables 3 – 6. Finally, the proposed system is based on a pure image generation using the two proposed algorithms, hiding and extraction. Finally, QR code image is not suspicious as it is considered a well-known image.

In future, more OSNs [31-34] can be used as a communication channels used for transmitting the secret message. Also, image retrieval [35, 36] can play a vital role in generating the new natural images used as stego images for coverless steganography. Different data types, such as text audios, and videos [37, 38], may be used for generating many robust coverless steganography systems.

References

Liu, H.H.; Lee, C.M. High-capacity reversible image steganography based on pixel value ordering. *J. Img. Vid. Proc.* **2019**, *2019*,1-15. DOI: org/10.1186/s13640-019-0458-z

Stanescu, D.; Stratulat, M.; Negrea, R.; Ghergulescu, I. Cover processing-based steganographic model with improved security. *Act. Polytech. Hung.* **2019**, *16*, 227-246. DOI: 10.12700/APH.16.1.2019.1.12

Zhang, X.; Peng, F.; Long, M. Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Trans. Multi.* **2018**, *20*, 3223-3238. DOI: 10.1109/TMM.2018.2838334

Baker, S.A.; Nori, A.S. Steganography in Mobile Phone over Bluetooth. *Int. J. Info. Tech. Bus. Manag.* **2013**, *16*, 111-117. DOI:10.1.1.1085.3522

Wiles, J.; Rogers, R. Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigators. Elsevier Inc., United States, USA, 2007; pp. 311-335. DOI: 10.1016/B978-1-59749-138-9.X5000-5

Elshazly, E.A.; Abdelwahab, S.A.S.; Fikry, R.M.; Zahran, O.; Elababyy, S.M.; El-Kordy, M. A Survey of Different Steganography Techniques. *Men. J. Elect. Eng. Res.* **2016**, *25*, 66-102. DOI: 10.21608/MJEER.2016.63662

Tan, Y.; Qin, J.; Xiang, X.; Zhang, C.; Wang, Z. Coverless Steganography Based on Motion Analysis of Video. *Sec. Comm. Net.* **2021**, *2021*, 1-16. DOI: org/10.1155/2021/5554058

Saad, A.H.S.; Mohamed, M.S.; Hafez, E.H. Coverless image steganography based on Jigsaw Puzzle Image Generation. *Comp. Mat. Cont.* **2021**, *67*, 2077-2021. DOI:10.32604/cmc.2021.015329

Hung, S.H.; Yao, C.Y.; Fang, Y.J.; Tan, P.; Lee, R.R.; Sheffer, A.;Chu, H.K. Micrography QR Codes. *IEEE Trans. Visual. Comp. Graph.* **2020**, *26*, 2834-2847. DOI: 10.1109/TVCG.2019.2896895

Chen, R.; Yu, Y.; Xu, X.; Wang, L.; Zhao, H.; Tan, H.Z. Adaptive Binarization of QR Code Images for Fast Automatic Sorting in Warehouse Systems. *Sens.* **2019**, *19*, 5466. DOI: org/10.3390/s19245466

Chang, J. An introduction to using QR codes in scholarly journals. *Sci. Ed.* **2014**, *1*, 113-117. DOI: 10.6087/kcse.2014.1.113

Cano, J.C. UbiqMuseum: A bluetooth and java based context-aware system for ubiquitous computing. *Wir. Per. Comm.* **2006**, *38*, 187–202. DOI: 10.1007/s11277-005-9001-x

Arulprakash, M.; Kamal, A.; Manisha, A. QR-Code scanner based vehicle sharing. *ARPN J. Eng. App. Sci.* **2018**, *13*, 3441-3448.

Johnson, M.; Dhanalakshmi, R. Predictive Analysis based Efficient Routing of Smart Garbage Bins for Effective Waste Management. *Int. J. Rec. Tech. Eng.* **2019**, *8*, 5733– 5739. DOI: 10.35940/ijrte.B2600.098319

Wu, J.; Liu, Y.; Dai, Z.; Kang, Z.; Rahbar, S.; Jia, Y. A coverless information hiding algorithm based on grayscale gradient co-occurrence matrix. *IETE Tech. Rev.* **2018**, *35*, 23-33. DOI: org/10.1080/02564602.2018.1531735

Zhou, Z.; Mu, Y.; Jonathan, Q.M. Coverless image steganography using partial-duplicate image retrieval. *Soft Comp.* **2019**, *23*, 4927-4938. DOI: 10.1007/S00500-018-3151-8

Zheng, S.; Wang, L.; Ling, B.; Hu, D. Coverless information hiding based on robust image hashing. Int. Conf. Intell. Comp. Springer, Cham, 7 August 2017, 1; pp. 536-547. DOI: 10.1007/978-3-319-63315-2_47

Wazirali, R.; Alasmary, W.; Mahmoud, M.M.; Alhindi, A. An optimized steganography hiding capacity and imperceptibly using genetic algorithms. *IEEE Acc.* **2019**, *7*, 133496-133508. DOI: 10.1109/ACCESS.2019.2941440

Li, S.; Chen, X.; Wang, Z.; Qian, Z.; Zhang, X. Data hiding in iris image for privacy protection. *IETE Tech. Rev.* **2018**, *35*, 34-41. DOI: 10.1080/02564602.2018.1520153

Cao, Y.; Zhou, Z.; Wu, Q.M.J.; Yuan, C. Coverless information hiding based on the generation of anime characters. *EURASIP J. Img. Vid. Proc.* **2020**, *36*, 1-15. DOI: org/10.1186/s13640-020-

00524-4

Zhou, Z.L.; Cao, Y.; Sun, X.M. Coverless information hiding based on bag-of-words model of image. *J. App. Sci.* **2016**, *34*, 527-536. DOI: 10.3969/j.issn.0255-8297.2016.05.005

Cao, Y.; Zhou, Z.; Sun, X.; Gao, C. Coverless information hiding based on the molecular structure images of material. *Comp. Mat. Cont.* **2018**, *54*, 197-207. DOI: 10.3970/cmc.2018.054.197

Cao, Y.; Zhou, Z.; Yang, C.; Sun, X. Dynamic content selection framework applied to coverless information hiding. *J. Inter. Tech.* **2018**, *19*, 1179-1185. DOI: 10.3966/160792642018081904020

Zou, L.; Sun, J.; Gao, M.; Wan, W.; Gupta, B.B. A novel coverless information hiding method based on the average pixel value of the sub-images. *Multi. Tools App.* **2019**, *78*, 7965-7980. DOI: 10.1007/s11042-018-6444-0

Luo, Y.; Qin, J.; Xiang, X.; Tan, Y.; Liu, Q.; Xiang, L. Coverless real-time image information hiding based on image block matching and dense convolutional network. *J. Real-Time Img. Proc.* **2020**, *17*, 1-11. DOI: 10.1007/s11554-019-00917-3

Zhou, Z.; Sun, H.; Harit, R.; Chen, X.; Sun, X. Coverless image steganography without embedding. Int. Conf. Comp. Sci. Springer, Cham, 13 August 2015, 1; pp. 123-132. DOI: 10.1007/978-3-319-27051-7_11

Zhang, Y.; Luo, X.; Guo, Y.; Qin, C.; Liu, F. Zernike moment-based spatial image steganography resisting scaling attack and statistic detection. *IEEE Acc.* **2019**, *7*, 24282-24289. DOI: 10.1109/ACCESS.2019.2900286

Edhah, B.S.; Alghazzawi, D.M.; Cheng, L. Secret communication on facebook using image steganography: experimental study. *Int. J. Comp. Sci. Info. Sec.* **2016**, *14*, 428.

Sahu, A.K.; Swain, G. A novel n-rightmost bit replacement image steganography technique. *3D Res.* **2019**, *10*, 1-18. DOI: 10.1007/s13319-018-0211-x

Xie, D.; Ren, J.; Marshall, S.; Zhao, H.; Li, H. A new cost function for spatial image steganography based on 2d-ssa and wmf. *IEEE Acc.* **2021**, *9*, 30604-30614. DOI: 10.1109/ACCESS.2021.3059690

Omar, A.; Mahmoud, T.M.; Hafeez, T.A.; Mahfouz, A. Multi-label arabic text classification in online social networks. *J. Info. Sys.* **2021**, *100*, 101785. DOI: org/10.1016/j.is.2021.101785

Omar, A.; Mahmoud, T.M.; Hafeez, T.A. Building online social network dataset for arabic text classification. Int. Conf. Adv. Mach. Learn. Techno. App. (AMLTA2018). Adv. Intell. Sys. Comp. Springer, Cham, Cairo, Egypt. 22 February 2018, 723; pp. 486-495. DOI: 10.1007/978-3-319-74690-6_48

Omar, A.; Mahmoud, T.M.; Hafeez, T.A. Comparative performance of machine learning and deep learning algorithms for arabic hate speech detection in OSNs. Int. Conf. Art. Intell. Comp. Vis. (AICV2020). Adv. Intell Sys Comp, Springer, Cham, Cairo, Egypt. 8 April 2018, 1153; pp. 247-257. DOI: 10.1007/978-3-030-44289-7_24

Mahmoud, T.M.; Hafeez, T.A.; Omar, A. A Highly Efficient Content Based Approach to Filter Pornography Websites. *Int. J. Comp. Vis. Img. Proc.* **2012**, *2*, 75-90. DOI: 10.4018/ijcvip.2012010105

Girgis, M.R.; Reda, M.S. A Study of the Effect of Color Quantization Schemes for Different Color Spaces on Content-based Image Retrieval. *Int. J. Comp. App.* **2014**, *96*, 1-8. DOI: 10.5120/16843-6699

Girgis, M.R.; Reda, M.S. Content-based Image Retrieval using Image Partitioning with Color Histogram and Wavelet-based Color Histogram of the Image. *Int. J. Comp. App.* **2014**, *104*, 17-24. DOI: 10.5120/18182-9073

Li, R.; Qin, J.; Tan, Y.; Xiong, N.N. Coverless Video Steganography Based on Frame Sequence Perceptual Distance Mapping. *CMC-Comp. Mat. & Cont.* **2022**, *73*, 1571-1583.

Mstafa, R.J. Reversible Video Steganography Using Quick Response Codes and Modified ElGamal Cryptosystem. *CMC-Comp. Mat. & Cont.* **2022**, *72*, 3349-3368.

الملخص العربي

عنوان البحث: إخفاء المعلومات باستخدام نظام الإخفاء بدون غلاف المعتمد على توليد الصور

الحسين صديق[٢]، محمد صلاح*[١]، جمال بحيري[١]، أحمد الحربي[١]
[١] قسم علوم الحاسب، كلية العلوم، جامعة المنيا، المنيا، مصر.
[٢] قسم علوم الحاسب، كلية الحاسبات والذكاء الاصطناعي، جامعة دمياط، دمياط، مصر.

يلعب توليد الصور دوراً مهماً لتصميم نظام قوى لإخفاء البيانات قادراً على مواجهة التحديات المختلفة لإخفاء المعلومات. يقترح البحث نظام لإخفاء البيانات مبنى على توليد الصور لديه إمكانية إرسال الرسائل السرية بطريقة آمنة. تشبه الصور التى تم توليدها بصور رمز الإستجابة السريعة QR code images وتم تسميتها فى البحث بإسم شبيه الـ QR code. يتكون النظام المقترح من عمليتين، تسمى العملية الأولى بعملية الرسالة السرية ويتم إستخدامها عند طرف مُرسل الرسالة وهى مسئولة عن توليد صورة شبيه الـ QR code من الرسالة السرية نفسها بإستخدام خوارزم الإخفاء. فى العملية الثانية، عملية إسترجاع الرسالة السرية، يتم إستخدامها عن طرف مُستقبل الرسالة لإسترجاع الرسالة السرية من صورة شبيه الـ QR code بإستخدام خوارزم الإسترجاع. فى النهاية، تم بناء النظام المقترح لإخفاء البيانات والذى يستخدم الخوازميات المقترحة. لتقييم كفاءة تلك الخوارزميات، تم تنفيذ التجارب العملية بإستخدام معايير تقييم مختلفة وهى Bit Error Rate (BER) و Success Rate (SR). لقد أكدت النتائج أن النظام المقترح أفضل من أنظمة الإخفاء التقليدية الأخرى محققاً أعلى سعة إخفاء ومستوى عالى من الحماية مقارنة بهم.