Designing A Novel Hybrid Algorithm for QR-Code Images Encryption and Steganography

Mohammad Soltani[1*], Amid Khatibi Bardsiri[2]

[1]Department of Computer Engineering, Kerman branch, Islamic Azad University, Kerman, Iran.
[2]Assistant professor, Department of Computer Engineering, Kerman branch, Islamic Azad University, Kerman, Iran.

* Corresponding author. Tel.: +989132981497; email: Soltani.mohammad.edu@gmail.com
Manuscript submitted April 23, 2018; accepted June 13, 2018.
doi: 10.17706/jcp.13.9.1075-1088

Abstract: Encryption is a method, for the protection of useful information, which is used as one of the security purposes and steganography is the art of hiding the fact that communication is taking place, by hiding information in other Information. In this article at first, plain text message as a security information is converted to the (Quick Response Code) QR-code image and then we proposed a new secure hybrid algorithm for the encryption and steganography of generated QR-code. In this article image encryption is based on two-dimensional logistic chaotic map and AES algorithm and steganography technique is based on LSB algorithm. In addition, Huffman algorithm has come out as the most efficient compression technique and we can use Huffman algorithm to compress encrypted QR-code. Experimental results show that the scheme proposed in this article has a high security and better QR-Code images encryption and steganography quality.

Key words: QR-code, encryption, decryption, steganography, two-dimensional logistic chaotic map, huffman's algorithm.

1. Introduction

One of the main tools for data protection, data confidentiality and user authentication is cryptography [1]. The best way to protect secret communication from unauthorized access is cryptography because it has a specific role for data protection [2], [3]. We can use encryption algorithm to prevent illegal access to multimedia data, whether personal, medical, military, and industrial or research [4]. Encryption for Multimedia data is different from the encryption of text data because multimedia data are heavily loaded. Due to the restriction like processor's capacity, bandwidth of communication networks and time, it's necessary to apply proper cryptography algorithms. Some of the articles have suggested cryptography algorithms using non-linear methods [5], [6]. However, some of these algorithms suffered from the absence of security [7]. For this reason, a new algorithm was proposed for the design of secure cryptography systems [8]. Chaos theory, a chapter of physics and math, it is concerned with systems whose dynamics show a very susceptible behavior towards the changes of initial values so that their future behaviors becomes unpredictable. These systems are called chaotic systems. They are, in fact, nonlinearity systems. This theory was expanded by Feigenbaum , Lorenz, Mandelbrot and Poincare [4]. An encryption algorithm mainly purposes to obtain a cipher text which is statistically indistinguishable by a real random subsequence. With limited computational ability, the bits of such plain texts can't be predicted by an

attacker [4]. Chaos system is a deterministic process but it appears to be a random one. These two specs of randomness and determinism made them suitable for designing encryption algorithms. The thought of using chaos theory dates back to 1949 after C.E.Shannon published his article entitled "The Theory of Communications of Security Systems" [4], [9]. Steganography is an algorithm for hiding and retrieving the high sensitive information in data conduction. In other words, steganography refers to the process of passing secret or confidential data in an image. In this process, an image is taken and secret message (payload) is set in that image and this image is passed to the sender. The sender can then extract the secret information from the image using the key provided by the sender [10]. The Least Significant Bit (LSB) is one of the main methods in spatial domain image steganography. In this article, a new technique of LSB steganography has been proposed which is an improvised version of one bit LSB algorithm [11]. In other to have more security we can use cryptography and steganography together as a hybrid algorithm. In this paper we suggested a new robust hybrid algorithm based on quick response code images encryption and steganography using Huffman's algorithm, chaos system and LSB algorithm. To increase security and prevent from unauthorized access to the contents of encrypted files, this hybrid algorithm can lead to further file theft Prevention and debarment from detecting contents of the secret file.

2. Related Works

Mamta Juneja *et al.*, [12] proposed a robust image Steganography. An algorithm based LSB insertion and encryption.

Z. Xiong *et al.*, [13] he has presented a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on Integer Wavelet transformation. B .Shiva Kumar *et al.*, [14] he has proposed the performance comparison of robust steganography algorithm based on multiple transformation techniques. This technique ensures more security than individual transformation techniques, which has excellent PSNR with high levels of security.

Sushil Kumar *et al.*, [15] he has presented a multi-layered secure, robust and high capacity image steganography algorithm. This algorithm achieved three layers of security, better in terms of imperceptibility, robustness and embedding capacity compared with corresponding algorithms based on DWT.

Shanjun Zhang *et al.*, [16] he has proposed a robust algorithm of embedding QR code into the DWT domain of divided blocks of the still image. This method was embedded information and extracted correctly even if the images are compressed to less percentage of the original according to the contents of the images.

Espejel-Trujillo *et al.*, [17] he has proposed a scheme allows using the security capacity of the VSS scheme together with robustness and easy acquisition of QR code. This method was performed ID-document authentication with secure and easy way without using sophisticated equipment.

3. Literature Review

3.1. QR-code

Quick Response code or QR-code is the trademark for a type of matrix barcode that allows to store a large volume of unique data and first designed for the automotive industry in Japan. A QR code uses four standardized encoding modes (alphanumeric, numeric, byte/binary, and kanji) to efficiently store data, extensions may also be used [18].

QR codes are two-dimensional (2D) so they can hold up to 7,089 numeric characters and up to 4,296 alphanumeric letterings worth of data. QR codes are free to create and to use and there are many inventive uses of a QR code that make it a very versatile technology.

The usual specifies 40 versions (sizes) of the QR code from the small 21 × 21 up to 177 × 177 modules in size. An improvement with QR code is also there relatively small size for a given amount of data The QR code is accessible in 40 different square sizes each with a user selectable inaccuracy correction level in four steps (referred to as inaccuracy correction level L, M, Q and H) [19].

3.2. Logistic Map

The logistic map was introduced first in 1845 by Verhulst [20] it is one of the simplest and thus more widely used chaotic maps. It is used as a model for the crowd growth of a species, it is expressed as a recurrence equation:

$$X_{n+1} = rX_n(1 - X_n) \tag{1}$$

This mapping relies on r and includes a simple square non-linear form. Through his discussions, Feigenbaum noticed this simple equation has other alternative responses, in addition to expected responses, which result simply by changing the parameter. If r value exceeds a certain limit, this system will show a chaotic response [4], [21]. The logistic equation is a simple non-linear equation with intricate dynamics [22]-[24]. Sample Bifurcation diagram logistic map is shown in Fig. 1.

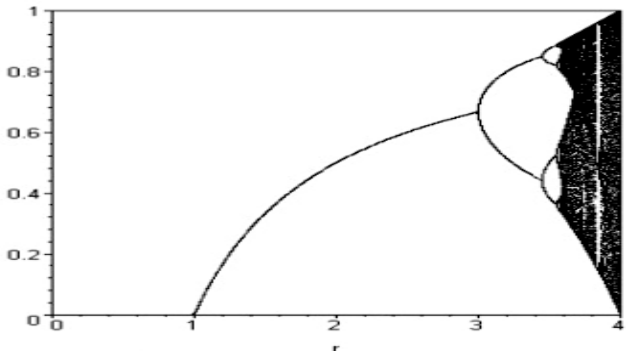


Fig. 1. Bifurcation diagram logistic map for r ∈ (1,4).

3.3. Two-Dimensional Logistic Map

The two-dimensional logistic map is researched for its complicated behaviors in image processing and image encryption [25], [26]. Two-dimensional logistic map has more complex chaotic behaviors than a one-dimensional logistic map [26]. Mathematically, this two-dimensional logistic map can be discretely defined as (2) where r is the system parameter and (x_i, y_i) is the pair-wise point at the *i* iteration [26].

$$X_{i+1} = r(3y_i + 1)X_i(1 - X_i)\ , y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \tag{2}$$

Fig. 2 shows the scatter plot of 30,000 points from the path [26], [27] of the two-dimensional logistic map using the parameter r=1.19 and the initial value (x_0, y_0) at (0.8309,0.3342). Therefore, the ith point on the trajectory can be determined by knowing (x_0, y_0, r, i), as Eq. (3) shows:

$$\begin{cases} X_i = \mathcal{L}_x^{2D}(i, r, x_0, y_0) \\ y_i = \mathcal{L}_y^{2D}(i, r, x_0, y_0) \end{cases} \tag{3}$$

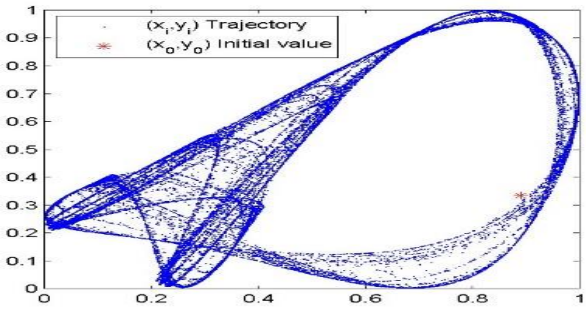


Fig. 2. A trajectory of the two-dimensional logistic map [26].

3.4. Least Significant Bit (LSB)

The Least Significant Bit (LSB) is one of the main algorithms in spatial domain image steganography. In the image pixel, LSB is the lowest significant bit in byte value. The LSB based image steganography embeds the secret in least significant bits of pixels' values of the cover image. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision.

Therefore, an altered image with low variations in colors will be invisible from the original by a human being, just by looking at it. In LSB technique just four byte of pixels are sufficient to hold one message byte. Rest of bits in the pixel remains the same [28]. Sample LSB algorithm is shown in Fig. 3.

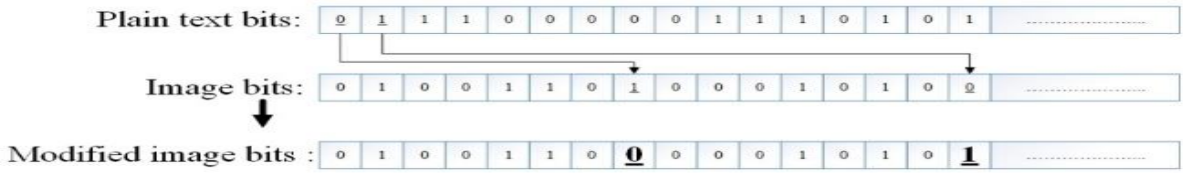


Fig. 3. Least significant bit example.

3.5. Base64

In this project we will use base 64 to ASCII text conversion and convert image to string. Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The term Base64 originates from a specific MIME content transfer encoding. Each base64 digit represents exactly 6 bits of data.

3.6. Huffman Coding

For using Huffman coding at first we must use quad tree decomposition and fractal theory [29]. Fractal Geometry has become an important branch of modern mathematics and nonlinear science, it has been widely used covering many branches of science and engineering. At now, among the studies of fractal compression encoding, there are two research focuses on the application of fractal on the field of image compression. The main problem is that the fractal encoding is taking too much time. Many approaches to reduce the encoding time has bad affection on the image quality after iteration, therefore the hybrid encoding system of combining fractal coding and other coding methods becomes an important direction of fractal methods. The quad tree approach divides a square image into four equal sized square blocks, and then tests each block to see if meets some criterion of homogeneity. If a block meets the criterion it is not divided any further, and the test criterion is applied to those blocks. This method is repeated iteratively until each block meets the criterion. The result may have blocks of several different sizes [30]-[32].

Fractal Compression Technique is defined based on following:

- Divides the original image using quad tree decomposition of threshold is 0.2, minimum. Dimension and maximum dimension is 2 and 64 respectively [29].

- Record the values of x and y coordinates, mean value and block size from Quad tree. Decomposition [29].
- Record the fractal coding information to complete encoding the image using Huffman. Coding and calculating the compression ratio [29].
- For the encoding image applying Huffman decoding to reconstruct the image and calculating PSNR [29].

3.7. MSE and PSNR

Mean square error (MSE): Mean square error is the difference between the original image and the encrypted image. This difference must be very high for a better efficiency [33]. Mathematically it is evaluated as follows:

$$\text{MSE} = (1/MN) * (\text{original image} - \text{encrypted image}) \tag{4}$$

For example, for 256*256 image the value of M=N=256. Peak signal to noise ratio (PSNR): Peak signal to noise ratio is the ratio of peak signal power to noise power. It is measured for image quality. For a good encrypted image, the value of PSNR must be low [33]. Mathematically it is evaluated as follows:

$$\text{PSNR} = 10\log_{10}\left(\frac{I2max}{mse}\right) dB \tag{5}$$

3.8. Information Entropy Analysis

The information entropy $H(X)$ is a statistical measure of uncertainty in communication theory [34]. It is defined as follows:

$$H(x) = \sum_{i=0}^{255}(\text{p}(x_i)log_2\text{p}(x_i)) \tag{6}$$

where X is a discrete random variable, $p(x_i)$ is the probability density function of the occurrence of the symbol x_i. We can get the perfect entropy $H(X)$ = 8.

4. Proposed Methodology

This project work proposes a data hiding in a generated QR code image which is compressed using Huffman algorithm and encrypted compressed image using two-dimensional logistic chaotic map and using Base64 conversion algorithm to convert encrypted image to string after that, generated string is encrypted using AES and encrypted text is hided in the input cover image using LSP technique So, the process is the identification of the secret message hided in the input cover image. The secret message will be transferred from sender to receiver where they access it. The secret message could be in the form of text data. Hiding of information techniques would be continually introduced. Also the degrees of complexity are increased. Thus the future malware related traffic could be harder to detect.

The process steps of the proposed methodology are defined based on following:

1- Read plain text.
2- Convert plain text to QR-code.
3- Read QR-code as a security image in the hybrid encryption algorithm.
4- Using Huffman algorithm to compress QR-code image.
5- Encrypt compressed Image using two-dimensional logistic chaotic map.
6- Using Base64 conversion algorithm and convert encrypted image to text.
7- Using AES algorithm and encrypt Base64 conversion result.
8- Using LSB steganography algorithm and embeds AES result in the cover image.

The schematic diagram of the proposed hybrid algorithm is shown in Fig. 4.

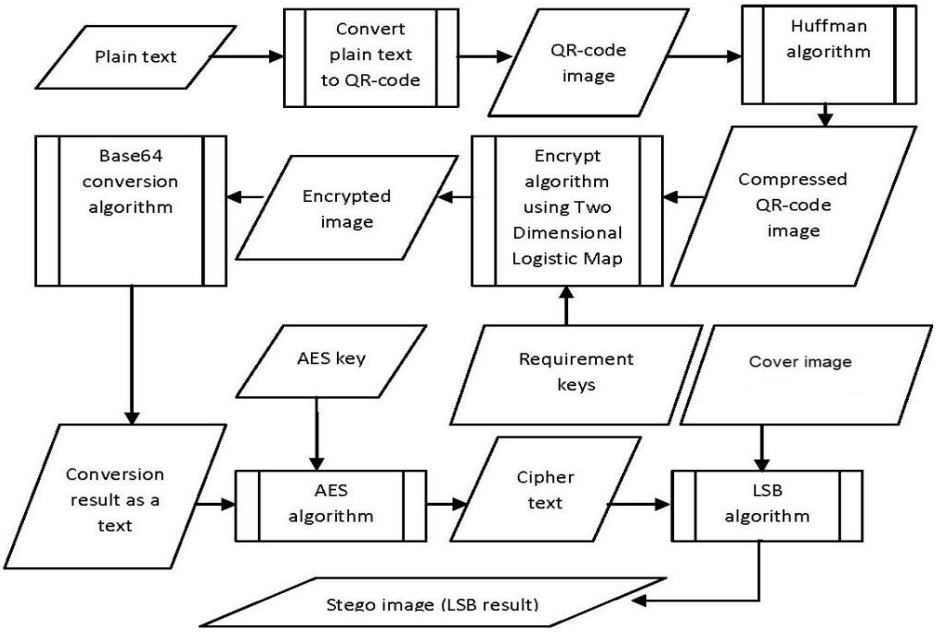


Fig. 4. Proposed hybrid algorithm model.

5. Implementation

In this article the features of our computer system used for implementation are defined based on following: Processor: Core i7 (2.10 GHz), RAM: 8 GB, Operating system: Windows 10, Simulation software and programming language: MATLAB, Visual studio and C#

5.1. Read Plain Text

In this step, security message is received as a plain text.

5.2. Convert Plain Text to QR-code

In this step, plain text is converted to QR-code image. In this article our sample plain text is "Secret message is so important". Plain text message Size is 30 bytes. Sample QR-code image is defined based on the Fig. 5.

Fig. 5. Sample QR-code image.

5.3. Huffman Algorithm

According to the main features of the Huffman algorithm, for compressing QR-code image at first we must use quadtree decomposition and fractal theory [27]. QR-code image compression method is shown in Fig. 6.

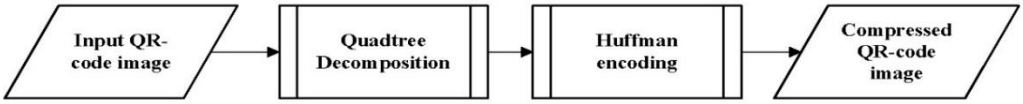


Fig. 6. The proposed fractal compression technique [29].

For sample QR-code image, performance analysis after compression is depicted in Table 1.

Table 1. Performance Analysis for Sample QR-code Image after Compression.

Test image	Message size (Byte)	Original size (Kb)	Compressed size (Kb)	Compression ratio	Compression Time (Second)	PSNR
Sample QR-code image	30	14.7	5	8.483122	8.024549	4.4303

5.4. Encrypt Algorithm Using Two-Dimensional Logistic Map

Although the two-dimensional logistic map has various behaviors according to different system parameters, in the paper we concentrate on the parameter interval r ∈ [1.1,1.19], where the system is chaotic. Fig. 7 shows the flowchart of the proposed image encryption algorithm using the two-dimensional logistic map. The internal loop is composed of 2-D logistic permutation, 2-D logistic diffusion and 2-D logistic transposition. Where each stage itself is an image cipher and they together form the permutation-substitution network [26], [27]. Similar to the encryption procedure, the decryption procedure is nothing but reversal of the order of processing using the decryption key, as Fig. 8 shows. The encryption process can be written as C=Enc(P,K), and the decryption process is P=Dec(C,K). All of the sub algorithms like, 2D Logistic sequence generator, 2D Logistic permutation, 2D logistic diffusion and 2D logistic transposition are defined in the Fig. 7 and Fig. 8.

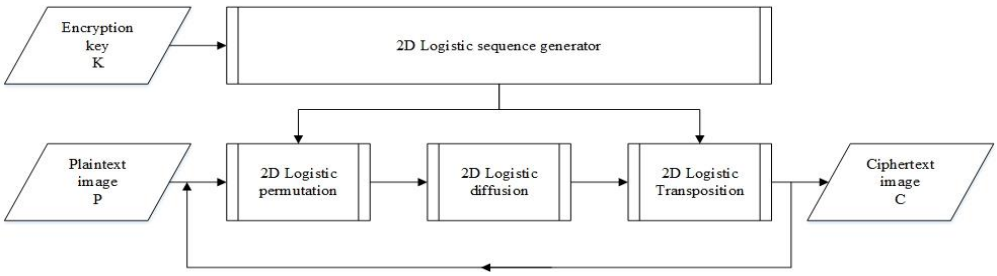


Fig. 7. The flowchart of the proposed image encryption method using the two-dimensional logistic map [26].

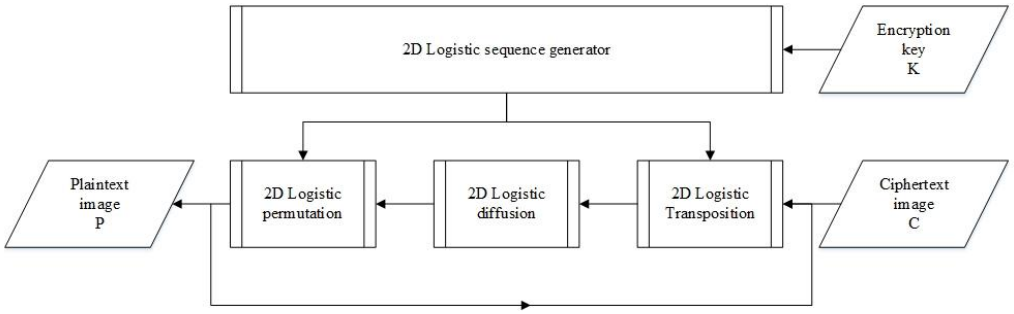


Fig. 8. The flowchart of the proposed image decryption method using the two-dimensional logistic map [26].

According to the main features of the Huffman algorithm and encryption algorithm, QR-code histogram, correlation and another parameter are defined based on following:

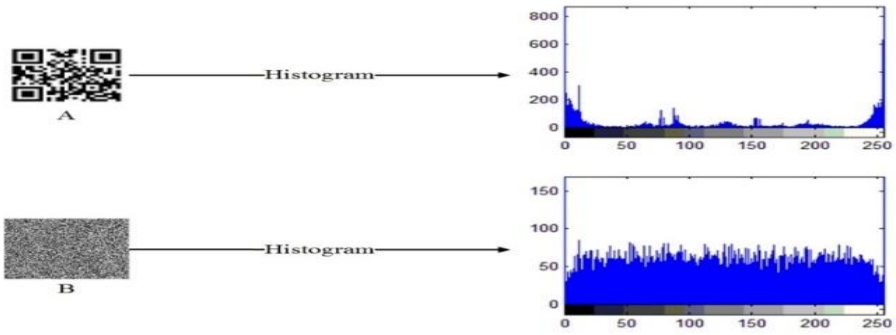


Fig. 9. A: QR-code after compression and its histogram, B: Compressed QR-code image after encryption and its histogram.

According to the Fig. 9, encrypted QR-code histogram analysis is one of the straightest methods of show the image cryptography quality. Since a good image encryption algorithm tends to encrypt a plain text image and it is desired to see a uniformly distributed histogram for a cipher text image [26]. The high information redundancy is one nature of the digital image data and thus it is desired to break the high correlation between neighbor pixels. In statistics, the auto-correlation Ra of a signal X describes the correlation between the signal X and its delayed version. The auto-correlation function Ra(0) is defined in Eq. (7), where the variable d is the time difference between the original signal and its delayed version, μ is the mean value defined by Eq. (8), and σ is the standard deviation defined by Eq. (9); the definition of mathematical expectation is given in Eq. (10) [26].

$$R_q(d) = E\left[\frac{(X_t-\mu)(X_{t+d}-\mu)}{\sigma*\sigma}\right] \quad (7)$$

$$\mu = E[x] \quad (8)$$

$$\sigma = \sqrt{E[[(X-\mu)]^2]} \quad (9)$$

$$E[x] = \sum_{i=1}^{N} \frac{Xi}{N} \quad (10)$$

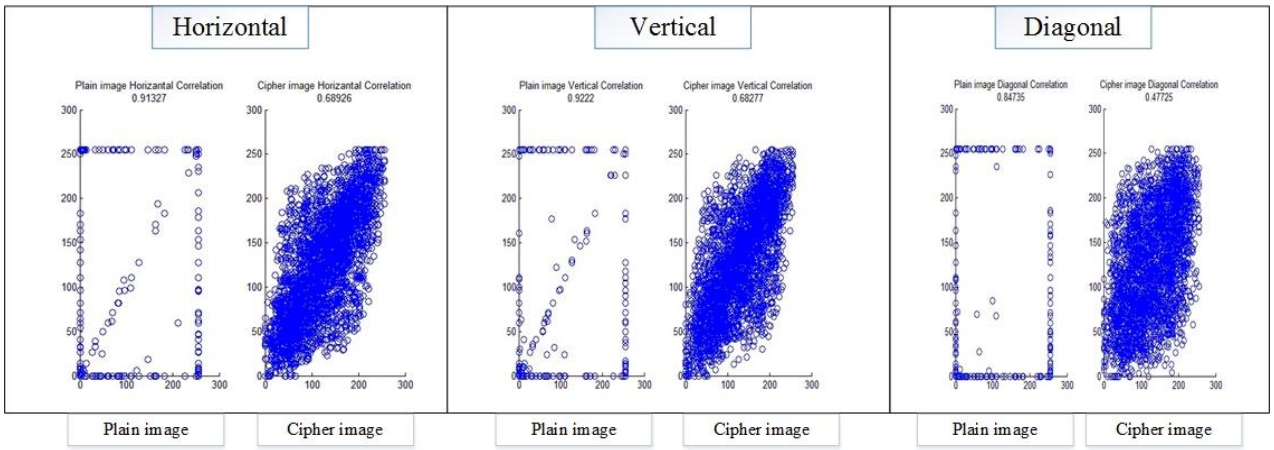


Fig. 10. Horizontal, vertical and diagonal correlations of QR-code after compression and using encryption algorithm.

The closer to zero this correlation coefficient is, the weaker the relationship between the original signal and its delayed version. In the adjacent pixel auto-correlation (APAC) test, X_t is then the pixel sequence of the test image and X_{t+d} is a corresponding adjacent pixel sequence, when d = 1. Since image pixel sequence can be extracted with respect to the horizontal, vertical, and diagonal directions, the APAC test scores are

also composed of three directional values [26].

According to the spatial relation of a pixel and its adjacent pixel, the APAC test can be applied for QR-code to all three directions (i.e., horizontal, vertical, and diagonal). According to the Fig. 10 each of the vertical, horizontal and diagonal values are defined based on following:

Table 2. Vertical, Horizontal and Diagonal Values of Sample QR-code Image after Compression and Using Encryption Algorithm

Image name	After compression		
	Vertical	Horizontal	Diagonal
cipher image	0.68277	0.68926	0.47725
Plain image	0.9222	0.91327	0.84735

According to the MSE and PSNR definition and Table 3, MSE value and entropy value of the compressed QR-code image is higher than Original QR-code image and PSNR value of the compressed QR-code image is lower than Original QR-code image.

Table 3. Performance Analysis for Sample QR-code Image after Encryption

Test image	Message size (Byte)	Size (kb)	Size after encryption (kb)	Time taken for encryption (Second)	MSE	PSNR	Entropy
Original QR-code image	30	14.7	36	122.358502	21.0965079803467e+003	4.88869786630627e+000	6.484229556477011
Compressed QR-code image (Ours method)	30	5	9.22	26.334959	21.1266705017090e+003	4.88249301897496e+000	7.875968738937592

For more information, this algorithm is tested with sample secret message of different sizes (103 bytes to 530 bytes) and the result is shown in Table 4.

Table 4. Entropy Analysis for Sample QR-code Image after Encryption.

Test image	Message size (Bytes)	Entropy
Original QR-code image	103	6.784829505472001
Compressed QR-code image (Ours method)	103	7.875722066089445
Original QR-code image	201	6.831969524747688
Compressed QR-code image (Ours method)	201	7.878526960921665
Original QR-code image	530	6.843320724861161
Compressed QR-code image (Ours method)	530	7.871955954738034

According to the Table 4 and entropy analysis, Compressed QR-code image entropy is higher than Original QR-code image entropy.

5.5. Base64 Conversion Algorithm

According to proposed hybrid algorithm model we must convert encrypted image to text. For convert encrypted image to Base64 string or text, at first we must convert it to byte array and then convert byte

array to Base64 string.

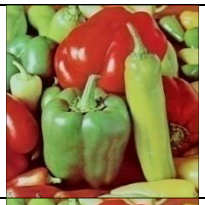
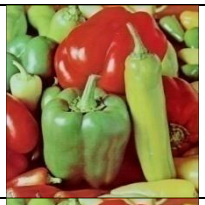
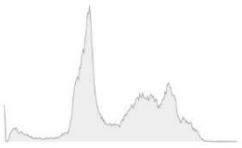
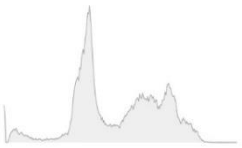
5.6. AES Encryption Algorithm

AES (Acronym of Advanced Encryption Standard) is a symmetric encryption algorithm and AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. According to proposed hybrid algorithm model we must encrypt Base64 result by using AES algorithm.

5.7. LSB Steganography Algorithm

Cryptography and steganography together provide a higher security level to the secret data. In the proposed hybrid algorithm after AES encryption we use LSB steganography algorithm and embed cipher text (AES result) in the cover image. For encrypted QR-code image, steganography Analysis is depicted in Table 5.

Table 5. Performance Analysis Encrypted QR-code Image after Steganography (Cover Image Size for both of the Original QR-code Image and Compressed QR-code Image is 20 Kb)

Encrypted image	**Message size (Byte)**	**QR-code Size (Kb)**	**Cover image (256 * 256)**	**Stego image (256 * 256)**	**Size of the stego image (Kb)**	**Histogram**
Original QR-code image	30	36			268	
Compressed QR-code image	30	9.22			258	

6. Compare the Proposed Hybrid Algorithm with Another Algorithm

Comparison of results of different hybrid techniques is depicted in Table 6.

Table 6. Comparison of Results of Different Hybrid Techniques

Encrypted image	**Message Size (Byte)**	**Stego image (512 * 512)**	**PSNR**	**MSE**
QR-code image in the [35]	103		52.585	0.601
Original QR-code image	103		51.1413	0.5000

Compressed QR-code image (Our method)	103		58.8274	0.0852
QR-code image in the [35]	201		52.587	0.601
Original QR-code image	201		54.5091	0.2302
Compressed QR-code image (Our method)	201		54.5093	0.2301
QR-code image in the [35]	530		52.586	0.601
Original QR-code image	530		51.1479	0.4992
Compressed QR-code image (Our method)	530		52.743	0.4991

According to the Table 6, in this article analysis of LSB algorithm has been successfully implemented & results are delivered. From the result it is the clear that PSNR is high and MSE is low in LSB based steganography.

In the steganography algorithm like LSB, it is better that MSE parameter of the cover image was less than previous state and it is better that PSNR parameter of the Cover image was more than previous state [36]. This new hybrid algorithm indicates that its performance is more powerful of steganography algorithm. This case in clearly shown in Table 6.

7. Conclusions

In this paper we suggested a new robust and secure Hybrid QR-code image encryption algorithm based on Huffman's algorithm, chaos system and LSB algorithm.

Briefly mention the performed task in each section of the paper:

Section 1 is introduction.

Section 2 discusses the related work about hybrid image encryption.

Section 3 is Literature review and this section discusses QR-code image, Logistic map, Two-Dimensional

Logistic Map, Least Significant Bit, Base64 conversion, Huffman coding and MSE and PSNR definition.

Section 4 is a summary about proposed Methodology.

Section 5 discusses all of the parts in the new hybrid algorithm.

According to the proposed algorithm, advantages of the new hybrid algorithm are defined base on following:

1- By encrypt QR-code image we can encrypt more than 7000 numbers or more than 4200 Alphanumeric characters jus as a QR-code image and use cryptography (Two-Dimensional Logistic Map algorithm) and steganography (LSB algorithm) together.
2- Decrease size of the encrypted QR-code image by using Huffman algorithm.
3- Increase MSE and entropy values and reduce PSNR value after encrypt compressed QR-code.
4- In the steganography algorithm like LSB, it is better that MSE parameter of the cover image was less than previous state and it is better that PSNR parameter of the Cover image was more than previous state. This new hybrid algorithm indicates that its performance is more stronger of steganography algorithm.
5- Time taken for encrypt compressed QR-code is lower than encrypt original QR-code.
6- After compression algorithm, entropy value of encrypted QR-code will be increased.
7- Size of the stego image for compressed QR-code is lower than size of the stego image for original QR-code and both of the stego images has a same histogram.

8. Future Work

The future work will be possible to make deeper hybrid algorithm in order to use new encryption and steganography techniques together to increase MSE value, decrease PSNR value, increase entropy value and flat histogram for encrypted image.

References

[1] Cryptography, o. (2013). *Theory and Practice of Cryptography and Network Security Protocols and Technologies.*

[2] Sheeraz Arif, A. S. (2011). Security key generation algorithm for user identification in voice over IP (VOIP) networks. *Journal of Basic and Applied Scientific Research, 1(12),* 3143-3148.

[3] Soltani, M. (2013). A new secure cryptography algorithm based on symmetric key encryption. *J. Basic Appl. Scient. Res, 3(7),* 465-472.

[4] Shu-Jiang, X., *et al*. (2008). A novel image encryption scheme based on chaotic maps. *Proceedings of 9th International Conference on Signal Processing, ICSP 2008.*

[5] Wang, Y., & Li, T. (2010). Study on image encryption algorithm based on arnold transformation and chaotic system. *Proceedings of International Conference on Intelligent System Design and Engineering Application (ISDEA).*

[6] Sharma, M., & Kowar, M. K. (2010). *Image Encryption Techniques Using Chaotic Schemes: A Review.*

[7] Li, C., *et al.* (2009). On the security defects of an image encryption scheme. *Image and Vision Computing, 27(9),* 1371-1381.

[8] Guardeño, D. A. (2009). Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems. *Universidad Politécnica de Madrid.*

[9] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal, 28(4),* 656-715.

[10] Kaur, A., Kaur, R., & Kumar, N. (2015). A review on image steganography techniques. *International Journal of Computer Applications, 123(4).*

[11] Champakamala, B., Padmini, K., & Radhika, D. (2013). Least significant bit algorithm for image steganography. *International Journal of Advance Computer Technology, 3(4)*, 34-38.

[12] Khare, A., Kunari, M., & Khare, P. (2010). Efficient algorithm for digital image steganography. *Journal of Information Science, Knowledge and Research in Computer Science and Application,* 1-5.

[13] Luo, L., *et al.* (2010). Reversible image watermarking using interpolation technique. *IEEE Transactions on Information Forensics and Security, 5(1),* 187-193.

[14] Kumar, K. S., *et al.* (2011). Performance comparison of robust steganography based on multiple transformation techniques. *Int. J. Comp. Tech. Appl, 2(4),* 1035-1047.

[15] Muttoo, S., & Kumar, S. (2011). A multilayered secure, robust and high capacity image steganographic algorithm. *World of Computer Science and Information Technology Journal, 6,* 239-246.

[16] Zhang, S., & Yoshino, K. (2008). *DWT-Based Watermarking Using QR Code.*

[17] Espejel-Trujillo, A., *et al.* (2012). Identity document authentication based on VSS and QR codes. *Procedia Technology, 3,* 241-250.

[18] Wave, D. (2010). QR code features. Retrieved from: www.QRCode. com

[19] Ramesh, M., Prabakaran, G., & Bhavani, R. (2014). QR-code image steganography. *Proceedings of the second International Conference on Emerging research in Computing, Information, Communication and Applications*.

[20] Weisstein, E. W. (1845). Logistic equation. *MathWorld.*

[21] Hashemi, S. M. (2009). Chaos and its application in engineering. *AlU Publication Tehran.*

[22] Fard, E. B., & Atani, R. E. (2013). A novel image encryption method based on chaotic maps. *Proceedings of 2013 3th International Conference on Computer and Knowledge Engineering (ICCKE).*

[23] Schuster, H. G., & Just, W. (2006). *Deterministic Chaos: An Introduction.* John Wiley & Sons.

[24] Afraĭmovich, V. S., & Hsu, S. B. (2003). Lectures on chaotic dynamical systems. *American Mathematical Soc.*

[25] Jha, Y., Kaur, K., & Pradhan, C. (2016). Improving image encryption using two-dimensional logistic map and AES. *Proceedings of 2016 International Conference on Communication and Signal Processing (ICCSP).*

[26] Wu, Y., *et al.* (2012). Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging, 21(1),* 013014.

[27] Young, L. S. (1982). Dimension, entropy and lyapunov exponents. *Ergodic Theory and Dynamical Systems, 2(1),* 109-124.

[28] Kumar, D.A.P., *et al.* (2016). Data hiding using LSB with QR code data pattern image. *International Journal of Science Technology & Engineering, 2(10).*

[29] Veenadevi, S., & Ananth, A. (2012). Fractal image compression using quadtree decomposition and huffman coding. *Signal & Image Processing, 3(2),* 207.

[30] Liu, B., & Yan, Y. (2010). An improved fractal image coding based on the quadtree. *Proceedings of 2010 3rd International Congress on Image and Signal Processing (CISP).*

[31] Yu, H., *et al.* (2010). Based on quadtree fractal image compression improved algorithm for research. *Proceedings of 2010 International Conference on E-Product E-Service and E-Entertainment (ICEEE).*

[32] Kamran, M., Sipra, A. I., & Nadeem, M. (2010). A novel domain optimization technique in Fractal image Compression. *Proceedings of 2010 8th World Congress on Intelligent Control and Automation (WCICA).*

[33] Srivastava, R., & Singh, O. (2015). Performance analysis of image encryption using block based technique. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 4(5),* 4266-4271.

[34] Wu, Y., Noonan, J. P., & Agaian, S. (2011). A novel information entropy based randomness test for image encryption. *Proceedings of 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC).*

[35] Rani, M. M., & RosemaryEuphrasia, K. (2016). Data security through QR code encryption and steganography. *Advanced Computing: An International Journal (ACIJ), 7(1/2),* 1-7.

[36] Kamdar, N. P., Kamdar, D. G., & Khandhar, D. N. (2013). Performance evaluation of lsb based

steganography for optimization of psnr and mse. *Journal of Information, Knowledge and Research in Electronics and Communication Engineering, 2(2),* 505-509.

Mohammad Soltani was born in Kerman, Iran in May 1991. He is received his B.S degree in computer software engineering from Shahid Bahonar University, Kerman, Iran in 2015 and he is currently pursuing his M.S degree of information technology in the department of computer engineering at Islamic Azad University of Kerman, Iran. His research interests include image processing, cryptography, security and cloud computing. He was announced as the top young researcher in MAHANI Scientific Festival based on his scientific curriculum vitae (CV) and articles. He was also accepted as a young scientific scholar in the ministry of science, research and technology in Iran In addition he was accepted in the young researchers and elite club. The Scientific profile: www.linkedin.com/in/profile-mohammad-soltani

Amid Khatibi Bardsiri received his B.S degree in computer software engineering from Shahid Bahonar University, Kerman, Iran in 2008, and his M.S degree in software engineering from Islamic Azad University, Tehran, Iran, in 2010. He received his PhD in science and research branch of Islamic Azad University, focusing on software metrics and measurement in 2015. He published about 100 research papers in international journals and conference proceedings. His areas of research include information systems engineering, software development, software metrics, grid computing, and cloud computing.