Indonesian Journal of Electrical Engineering and Computer Science
Vol. 19, No. 3, September 2020, pp. 1428~1435
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v19.i3.pp1428-1435

Survey on computational intelligence based image encryption techniques

Thirumalaimuthu T. Ramanathan[1], J. Hossen[2], S. Sayeed[3], J. Emerson Raja[4]
[1,3]Faculty of Information Science and Technology (FIST), Multimedia University (MMU), Malaysia
[2,4]Faculty of Engineering and Technology (FET), Multimedia University (MMU), Malaysia

Article Info

Article history:

Received Feb 2, 2020
Revised Mar 17, 2020
Accepted Apr 6, 2020

Keywords:

Fuzzy logic
Genetic algorithm
Image encryption
Neural network
Visual cryptography

ABSTRACT

Image encryption is an important area in visual cryptography that helps in protecting images when shared through internet. There is lot of cryptography algorithms applied for many years in encrypting images. In the recent years, artificial intelligence techniques are combined with cryptography algorithms to support image encryption. Some of the benefits that artificial intelligence techniques can provide are prediction of possible attacks on cryptosystem using machine learning algorithms, generation of cryptographic keys using optimization algorithms, etc. Computational intelligence algorithms are popular in enhancing security for image encryption. The main computational intelligence algorithms used in image encryption are neural network, fuzzy logic and genetic algorithm. In this paper, a review is done on computational intelligence-based image encryption methods that have been proposed in the recent years and the comparison is made on those methods based on their performance on image encryption.

Corresponding Author:

Thirumalaimuthu T. Ramanathan,
Faculty of Information Science and Technology,
Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia.
Email: 1181402216@student.mmu.edu.my

1. INTRODUCTION

Mathematical modeling can be ineffective for some complex real-world problems, and in such cases, computational intelligence can support. Computational intelligence is a subfield of artificial intelligence that deals with numerical data based on nature-inspired computational methodologies which has the ability to learn, reason, and optimize the data. The computational intelligence mainly includes artificial neural network (ANN), fuzzy logic and genetic algorithm.

ANN is an information processing paradigm that works similar to how the brain process information. Artificial neurons are interconnected elements of ANN architecture that process information simultaneously. ANN learns from sample data and use their pattern for reasoning. A neuron receives several signals from its input links, computes a new activation level and sends it as an output signal through the output links. The input of neuron can be raw data or outputs of other neurons. The output can be either a final solution to the problem or an input to other neurons. The neuron uses the following transfer or activation function [1]:

$$X = \sum_{i=1}^{n} x_i w_i \quad (1)$$

$$Y = \begin{cases} +1 \; if \; X \geq \theta \\ -1 \; if \; X < \theta \end{cases} \quad (2)$$

where X is the net weighted input to the neuron, x_i is the value of input i, w_i is the weight of input i, n is the number of neuron inputs, and Y is the output of the neuron. The neuron computes the weighted sum of the input signals and compares the result with a threshold value, θ. If the net input is less than the threshold, the neuron output is -1. But if the net input is greater than or equal to the threshold, the neuron becomes activated and its output attains a value +1. ANN produces output based upon the input and activation function.

Fuzzy logic is a part of fuzzy set theory [2] that uses degrees of membership and degrees of truth for representing the knowledge. Fuzzy logic is a multi-value logic that uses the continuum of logical values between 0 (completely false) and 1 (completely true) [3]. Fuzzy logic is used to deal with uncertain data where the exact value of data is unclear. A fuzzy logic is processed by fuzzifying all the input values into fuzzy membership functions, then it has a rulebase to compute the fuzzy output functions, then the "crisp" output values is generated by de-fuzzifying the fuzzy output functions.

Genetic algorithm is a famous optimization algorithm based on the concept of Darwin's theory of evolution [4] with the aim of finding the best solutions to a given computational problem that maximizes or minimizes a particular function. The genetic algorithm has the following steps: at first, the initial population is generated using random or default values, then fitness function is applied on each member of the population, then a fittest member of the population is generated based on the fitness function. The above process is repeated until a desired number of iterations have passed and generates the best members of the population [5].

Nowadays large multimedia information, such as color images, audio and video are stored and shared through the internet every moment [6]. It is important to protect these data from unauthorized access. Providing security to digital images is still a research challenge. There are various types of technologies to support image content protection such as data hiding [7], watermarking [8], and encryption [9]. Image encryption technology is an efficient method to encrypt images using cryptography that transforms the meaningful images into an unrecognized one [10, 11]. Image encryption is seriously considered in image security as private images are one of the confidential data that are transferred over internet, for example, the medical images in healthcare industry. Several cryptographic approaches are proposed to improve the image encryption methods such as to improve key size, key sensitivity and to resist all possible hackers' attacks. The traditional cryptographic algorithms are not enough to achieve very high level of security in image encryption and so artificial intelligence techniques are applied to improve image encryption methods in the recent years. The computational intelligence algorithms improve the image encryption methods by generation of random keys, and can further strengthen the image encryption. For example, chaotic systems are nonlinear dynamical systems that depend on initial condition and pseudo random behavior. Chaotic systems are applied in cryptography for many years. Computational intelligence algorithms have been combined with chaos functions in the recent years to improve the image encryption process and to attain high security level. In this paper, a review is done on research papers that use computational intelligence algorithms for image encryption.

So far, there has been many reviews done by researchers on image encryption methods, but there is no recent work in reviewing and highlighting the artificial intelligence-based methods on image encryption. The objective of this paper is to review and compare the latest computational intelligence-based encryption methods to find their strength and weakness in image encryption. This paper reviews how the ANN models, fuzzy logic and genetic algorithm are used in various image encryption methods to enhance the encryption process. The review on computational intelligence-based image encryption methods will motivate the visual cryptography researchers to improve and innovate multiple intelligent encryption approaches for image security. In the below sections, the research papers that uses computational intelligence algorithms for image encryptions process are reviewed and comparison is made among those papers based on their performance.

2. REVIEW ON COMPUTATIONAL INTELLIGENCE BASED IMAGE ENCRYPTION

In 2013, Afarin and Mozaffari [12] provided an encryption method that includes two stage which are substitution stage and modification stage. The pixels positions of the input image are changed to minimize the correlation between adjacent pixels in the substitution stage. Then, in the modification stage, the pixel values are modified to encrypt the input image. The genetic algorithm with binary chromosomes is used to achieve the both stages. Local binary pattern (LBP) is applied to produce these binary patterns for substitution stage and bit plane slicing (BPS) is applied to get binary chromosomes for modification stage. In their proposed method, the rows and columns of input image are the initial population of the genetic algorithm. In the initial population, a random generator having predefined key is applied as an alternative to subjective selection of parents and average of transition from 0 to 1 and 1 to 0 in LBP image and histogram uniformity is considered as the fitness function in genetic algorithm in substitution and modification stages respectively. The author mentioned that their proposed method is sensitive to the keys and small deformation in them does not restore the original image.

In 2013, Mahmood et al. [13] presented asymmetric encryption approach for medical images. Their approach uses genetic algorithm. Based on pixel intensity and entropy estimation, the medical images are divided into number of parts. Their selective encryption method involves use of various encryption algorithms with different key lengths for encryption to manage the encryption processing time. In their approach, the low processing algorithm such as the Gold code [14] is used to encrypt the low information regions, standard algorithm such as AES [15] is used to encrypt the high information regions and the algorithms such as DES [16] or Blow Fish [17] is used to encrypt the remaining regions. The author stated that the result of their proposed approach is fast and robust that fits to the information content of each individual image.

In 2014, Wang and Xu [18] presented a selection-crossover-mutation architecture for confusion and diffusion of image. According to their proposed approach, individual and gene in genetic algorithm are each pixel and bit of image. In their proposed selection-crossover-mutation architecture, the first phase is selection phase that uses "Monte Carlo" [19] method to select two individuals randomly as per the chaotic sequences which is generated by intertwining logistic map [20]. The second phase is crossover phase which cross the selected individuals and use crossover operator to swap their genes. And the final phase is the mutation phase which randomly alters the genes of the individuals. The author pointed out that their proposed structure has large key space and suitable to image encryptions.

In 2015, Das et al. [21] proposed an encrypted technique that consists of several steps for encrypting images. In their technique, initially a key set is formed depending on sixteen random characters and a big number. The next step consists of diffusion of images. The genetic algorithm based on ring crossover and order changing mutation is used to compute the key set and diffused image. The logical operation among the diffused image and key is used to obtain the encrypted image.

In 2015, Saranya et al. [22] proposed an encryption algorithm based on chaotic function [23], deoxyribonucleic acid (DNA) sequencing [24] and genetic algorithm. According to their proposed algorithm, the logistic map function is used to produce a chaotic sequence of desired length. A secret key is used to compute the initial value of logistic map function. The image encryption is done using chaotic sequences and several DNA masks. The finest mask for encryption is obtained by genetic algorithm. The author indicated that their proposed algorithm shows high entropy, low correlation between pixels and has resistance to various types of attacks.

In 2016, Chai et al. [25] proposed an encryption algorithm using genetic recombination and 4D memristive hyperchaotic system [26]. According to the proposed algorithm, the input image is broadened into two images parts made by selected four bit-planes and are diffused at bit plane level. The genetic recombination is used to reconstruct the blended bit planes and key streams. Then the standard diffusion is conducted to get the encrypted images. In their algorithm, the pseudorandom sequences in every phase are produced by 4D hyper-chaotic scheme.

In 2016, Dridi et al. [27] proposed an algorithm that employs two encryption processes. The first one uses chaotic map and the second one is based on ANN and chaotic system. According to their proposed algorithm, first, the input image is XORed by a main key to get the encrypted image. The key is produced by a loop of two chaotic maps. Then, a logistic map is created to generate parameters of the ANN. At last, by using the ANN and chaotic system, the encrypted image is further encrypted to get the final encrypted image.

In 2016, Lin et al. [28] proposed encryption scheme using Latin square and cellular neural network (CNN) [29]. According to the proposed scheme, the pixel values substitution is made in the input image by using Latin squares and CNN. Then, the substituted image is split into number of blocks using Latin squares. Then, the encrypted image is obtained by scrambling every block.

In 2016, Slimane et al. [30] proposed a light weight method to encrypt and decrypt image using a combination between chaotic attractor of Henon [31] and Hopefield neural networks (HNN) [32]. HNN is a completely linked neural network that shows pseudo-randomness based on the weight matrix. Their proposed method consists of two main process, confusion and diffusion stage using chaotic neural key. The first stage of confusion is computed by permuting the pixel position by combination of chaotic attractor and neural networks, the second stage is the modification of pixels values controlled by the same chaotic sequence used in the fist process with a keystream and the number of iterations for confusion and diffusion process. The author mentioned that their proposed method shows better speed in image encryption.

In 2016, Wang [33] proposed an encryption algorithm to enhance the process of scrambling encryption [34] using genetic super chaos. Their proposed algorithm produces outcome of the image scrambling which depends not only on the chaotic sequence constructed by the initial key but is also based on the image characteristics itself, which provides the adaptive features to some degree. Their proposed algorithm has a clear feedback mechanism for diffusion in the encryption process. The author mentioned that their algorithm improves the ciphertext attack resistance.

In 2017, Hu et al. [35] proposed an encryption algorithm using CNN chaotic system and matrix transformation. The encryption key of their proposed algorithm is the initial state of CNN which produces 5D chaotic sequence. According to their algorithm, the image pixel values are modified by conducting XOR operation among the pixel values of the input image and modified chaotic sequence. And the cipher image is formed by a construction matrix which modifies the pixel positions. The author mentioned that their proposed algorithm shows powerful key sensitivity and great security.

In 2017, Norouzi and Mirzakuchaki [36] proposed an encryption approach using neural network-based scheme, CNN. According to their proposed approach, initially, the input image is evenly partitioned into four sub-images and a DNA sequence matrix is obtained for every sub-image. Then the encryption of every DNA sub-image is done by the hamming distance and DNA sequence operation. Then CNN is used for generation of pseudorandom key stream. Algebraic transformation is applied to the 256-bit key for deriving the initial conditions and parameters of CNN. At last, the chaotic sequence produced by CNN is used to change the pixel values and reduce the correlation among the adjacent pixels of the image. The author stated that their proposed approach is also suitable for encrypting audios and videos.

In 2017, Ratnavelu et al. [37] proposed an encryption method based on fuzzy cellular neural network (FCNN) [38]. FCNN is an extension of CNN with high level information processing ability, such as image perception of fuzzy systems. Integration of fuzzy set theory and CNN paradigm is used to obtain FCNN processing paradigm for finding uncertainties in each level of image processing. FCNN gives fuzzy operation abilities for each cell in CNN. According to their proposed method, each chaotic signal produced by FCNN is employed on every pixel of the input image to generate the encrypted image. The author mentioned that their proposed method shows high key sensitivity.

In 2018, Abbasi et al. [39] presented an encryption algorithm for digital grey images using genetic algorithm and lattice map function. A lattice map function is a dynamical system that models the behaviors of nonlinear systems which is used to qualitatively study the chaotic dynamics of spatially extensive systems. According to their proposed algorithm, in the first step, the initial value of logistic map function has been obtained from a 120-bit key using the proposed method, and then in the second step, the pixels of the original image were confused using the produced chaos sequence. In third step, the original image is encrypted using the lattice map function sequence obtained from the logistic map function in the previous image. This process continues with number of initial populations of the genetic algorithm. Then the finest encrypted image is obtained in each step of loop of genetic algorithm. The author indicated that their proposed algorithm shows high resistance to any statistical attacks.

In 2018, Das et al. [40] proposed an encryption technique which consists of three stages that uses pseudo random number generator, genetic algorithm and Arnold cat map [41] for image encryption. According to their proposed technique, initially every pixel of the input image is modified by employing crossover and mutation operators of genetic algorithm. A random sequence from logistic map selects the crossover points. Then, Arnold cat map is used to jumble the pixels of altered image. At last, the logical operation is performed among the altered image and random sequence to produce the encrypted image. The author indicated that their proposed technique has resistance to various types of attacks

In 2018, Das et al. [42] proposed a hybrid of particle swarm optimization (PSO) [43] and genetic algorithm approach to encrypt an image. The key is generated using genetic and PSO algorithm. The genetic algorithm produces different numbers and the elements of keyset are selected by using PSO. The logical operation among the image and key value generates the encrypted image. The author pointed out that their proposed approach is vey much effective for diffusion and confusion of pixels and is highly sensitive to any types of statistical attacks.

In 2018, Dey [44] proposed a grayscale image encryption concept using a confusing-diffusing architecture, irreducible polynomial, fuzzy operations and linear cryptanalysis [45]. In the proposed method, the irreducible polynomial is implemented to design the confusion - diffusion architecture that scrambles the pixel position of the image. The pixel intensities of the images are altered using the fuzzy operations, and then using linear cryptanalysis, the image is encrypted.

In 2018, Kaur and Kumar [46] proposed an encryption method based on beta chaotic map [47], nonsubsampled contourlet transform (NSCT) [48], and genetic algorithm. According to the proposed method, first, the NSCT is used to divide the original image into sub bands. Then, then coefficients of sub bands are encrypted by pseudo-random key generated by beta chaotic map. And the genetic algorithm is employed to discover the best parameter of beta chaotic map. Finally, the encrypted image is obtained by the inverse of NSCT.

In 2018, Kaur and Kumar [49] proposed an encryption technique that uses intertwining logistic map based on parallel non-dominated sorting genetic algorithm (NSGA) to encrypt the images. According to their proposed technique, the initial parameters of the intertwining logistic map are tuned by NSGA. The secret keys generated by the intertwining logistic map are improved by the Fourier-Mellin based matrix. Finally, the image

encryption is performed by the permutation and diffusion operations conducted on the original image utilizing the secret keys. The author mentioned that their proposed technique shows good computational speed.

In 2018, Maddodi et al. [50] proposed a method that integrates ANN, chaos based pseudorandom sequence generator and DNA based chaotic encryption algorithm for image encryption. A heterogeneous neural network based chaotic pseudo random generator is used to manage the pixel position permutation, DNA-based bit substitution and permutation method. The control parameters of chaotic functions in the neural network are dynamically updated to enhance the randomness of the generated chaotic sequence. The author stated that their proposed method enhances the statistical properties of the encrypted images.

In 2018, Mousa [51] proposed an iterative chaotic genetic-fuzzy encryption technique (C-GET) for the image encryption. The encryption phases of C-GET are chaotic map functions, fuzzy logic and genetic operations. According to the proposed technique, the input image is converted into bytes and into 2D matrix composed of 0 and 1. The confusion and diffusion of the matrix is performed using fuzzy and genetic operation. The chaos function is used to generate appropriate fuzzy members and fuzzy rules. The author pointed out that their proposed technique has large key space and provides multilayer protection levels against various attacks.

In 2018, Mozaffari [52] proposed an encryption method based on LBP, BPS and genetic algorithm. According to their proposed method, a set of binary images is obtained by the input image by using LBP and BPD techniques. Then, crossover and mutation operations of genetic algorithm are used to perform permutation and substitution stages. At last, the encrypted image is obtained by combining the scrambled bit planes. In their proposed method, a deterministic method with security keys is used instead of random population selection to strengthen the encryption. The author mentioned that their proposed method has high encryption speed.

In 2019, Dey and Paul [53] proposed ANN based scheme that encrypts a color image for secure image transmission. Their proposed scheme is divided into three steps, initially the input image is partitioned into RGB factors, and using the chaotic map, a random shuffle is done on these RGB factors to get the first encrypted image, then the first encrypted image is processed through the single-layer ANN to get the second encrypted image and finally the pixels of the second encrypted image are shuffled using the exclusive-or (XOR) operation to get the final encrypted image for transmission over insecure channel. Their proposed scheme can protect from several statistical attacks like plaintext attack, cipher text attacks, brute force attack, and birthday attack etc.

In 2019, Wang and Li [54] proposed an encryption algorithm that is based on chaotic-HNN. According to their proposed algorithm, the initial key processing is done using integration of chaotic map, logistic map and tent map [55]. The parameters of the Arnold map are obtained by a function transformation required for scrambling the image. Chaotic-HNN is used to produce the self-diffusion chaotic matrix. The scrambled image is XORed with the key to get the final cipher image. The author pointed out that their proposed algorithm has resistance to statistical attack methods.

3. COMPARISON OF REVIEWED METHODS

The intelligent image encryption methods reviewed above are analyzed through properties such as number of pixels changing rate (NPCR), unified average changing intensity (UACI), information entropy, correlation coefficients (CC), horizontal CC (HCC) and vertical CC (VCC) [56, 57].

The properties NPCR and UACI are used to measure the difference between the original image and encrypted image which are described mathematically as (3) and (4) [56].

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (3)$$

$$\text{UACI} = \frac{1}{W \times H} \times \left[\sum_{i,j} \frac{C(i,j) - C`(i,j)}{255}\right] \times 100\% \quad (4)$$

where W and H are width and height of the image, C and C` represent the encrypted image before and after one pixel of the original image is changed. If C(i,j) = C‘(i,j), then D(i,j) = 0, otherwise D(i,j) = 1.

The CC of the pixels are calculated according the following formula (5) and (6) [57].

$$r_{x,y} = \frac{E((x - E(x))\,(y - E(y)))}{\sqrt{D(x)D(y)}}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (5)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (6)$$

where x and y are grey-scale values of two adjacent pixels in the image, E(x), E(y) are the expectation of variable x and y respectively and D(x), D(y) are the variance of variable x and y respectively.

Information entropy concept evaluates the unpredictability and randomness of the grayscale images. The information entropy, H(S) is described as (7) [58].

$$H(S) = \sum_{i=0}^{2^L-1} P(S_i) log_2(1/P(S_i)) \quad (7)$$

where $P(S_i)$ is the probability of the source image S_i, and L is the sum of pixels of the image.

Table 1 shows NPCR, UACI, entropy, CC values and key space of the image encryption methods in the reviewed papers. The "NU" in the table indicates that those properties were not used in the reviewed papers for performance analysis. The algorithm showing highest NPCR, UACI, entropy and lowest CC values are considered as the best method for image encryption. Based on the comparison, it seems that most of the reviewed methods show good image encryption performance only with little difference in their outcomes. It can also be seen from the table that the key space of the reviewed image encryption methods is large enough to resist most known attacks like brute force attack. In most of the reviewed papers, the encryption processing time of the reviewed algorithms is not discussed which is obvious from their large key space values that it causes reduction in the encryption speed. The main drawback in having a large key space is that it decreases the encryption speed whereas the small key space leads to brute force attack. The reviewed computational intelligence-based image encryption algorithm should be improved to modify the key space according to the size and quality of image being encrypted such that it should increase the encryption speed and also resist any kind of attacks. As all of the reviewed image encryption methods are tested on a single image separately, the other research challenge found in the reviewed papers is whether these computational intelligence-based image encryption methods show the same level of performance for selective and multiple image encryption problems.

Table 1. Performance analysis of the reviewed papers

Reviewed Papers	NPCR	UACI	Information Entropy	CC, HCC, VCC	Key Space
Ref. [12]	NU	NU	7.9968	CC: -0.00058	2^{256}
Ref. [13]	0.9965	NU	7.9432	CC: 0.009	2^{256}
Ref. [18]	0.9960	0.3347	7.9993	HCC: −0.00113, VCC: −0.00179	larger than 10^{109}
Ref. [21]	NU	NU	7.9948	CC: 0.0093	2^{145}
Ref. [22]	0.9950	0.3565	7.9982	CC: -0.0012	2^{120}
Ref. [25]	0.9960	0.3328	7.9993	HCC: 0.0083, VCC: - 0.0046	2^{256}
Ref. [27]	0.9943	0.337	7.9992	CC: 0.00537	2^{325}
Ref. [28]	0.9961	0.3351	7.9968	NU	larger than 2^{795}
Ref. [30]	0 .9960	0.32942	7.9963	HCC: 0.0021, VCC: 0.0037	10^{64}
Ref. [33]	NU	NU	7.9786	HCC: 0.00038, VCC: 0.0209	larger than 10^{75}
Ref. [35]	0.9959	NU	7.9911	HCC: 0.0052, VCC: 0.0198	2^{30}
Ref. [36]	0.9961	0.3346	7.9980	CC: 0.0021	2^{256}
Ref. [37]	0.9995	0.3333	7.9977	CC: -0.7267	larger than 2^{900}
Ref. [39]	0.9970	0.3418	7.9994	HCC: 0.0015, VCC: 0.0009	2^{120}
Ref. [40]	NU	NU	7.9954	CC: 0.0048	2^{256}
Ref. [42]	NU	NU	7.9953	HCC: 0.0015, VCC: 0.0009	2^{256}
Ref. [44]	0.9974	0.3358	7.9993	HCC: 0.1696, VCC: 0.1325	2^{256}
Ref. [46]	0.9963	0.3341	7.9975	HCC: 0.0012, VCC: 0.0058	2^{26952}
Ref. [49]	0.9979	0.3351	7.9993	HCC: 0.0003, VCC: −0.0012	10^{42}
Ref. [50]	0.9961	0.2856	7.9976	HCC: −0.0026, VCC: 0.0023	2^{64}
Ref. [51]	0.0015	0.3153	7.9991	CC: 0.0059	2^{256}
Ref. [52]	0.9958	0.3308	7.9968	HCC: −0.00058, VCC:0.0048	2^{160}
Ref. [53]	0.9961	0.3352	7.9994	HCC: 0.1830, VCC: 0.1648	2^{32}
Ref. [54]	0.9960	0.3346	7.2926	HCC: 0.0036, VCC: 0.0083	larger than 2^{128}

4. CONCLUSION

This paper reviewed the latest research papers that use computational intelligence algorithms for image encryption. Based on the review, it can be concluded that the computational intelligence has the capability to fill the research gap found in cryptography-based image encryption methods. With the development of hacking techniques, the computational intelligence-based cryptography methods are effective to resist the latest cyber attacks. However, there are drawbacks in the reviewed papers. All of the reviewed image encryption methods were tested on single image separately. To encrypt bulk image data of different size simultaneously is still a research challenge. The performance of image encryption methods should be improved for dealing with images transmitted and shared through internet such as cloud computing environment. Bulk data images of different sizes in high definition format are being shared nowadays in

cloud environment which shows high correlation among pixels. In such a case, an improved hybrid intelligent technique needs to be modeled and incorporated with image encryption methods to learn and detect possible attacks for images depending upon their features and to optimize automatically the encryption algorithm based on the input images. For example, if high quality images are given, then the intelligent model should automatically increase the key size and pixel substitution methods for better security. Multi-agent system might address these challenges in such a way that assigning number of tasks to different agents such as predicting the possible attacks on the input images, generating random cryptographic keys based on the image size, controlling the size of secret key space, reasoning on how many encryption layers needed for the given image, etc. The possible future research work in intelligence-based image encryption area will be of design and development of multi-agent system that employs various intelligent encryption methods to encrypt multiple images simultaneously

REFERENCES

[1] S. Haykin, "Neural networks, a comprehensive foundation," *New Jersey: Prentice-Hall*, 1994.
[2] L. A. Zadeh, "Information and control," *Fuzzy sets*, vol. 8, pp. 338-53, 1965.
[3] V. Novák *et al.*, "Mathematical Principles of Fuzzy Logic," *Dordrecht: Kluwer Academic*, 1999.
[4] D. L. Hull, "Darwin and his critics: The reception of Darwin's theory of evolution by the scientific community," *Chicago: University of Chicago Press*, 1973.
[5] D. Whitley, "A genetic algorithm tutorial," *Statistics and computing*, vol. 4, no. 2, pp. 65-85, 1994.
[6] K. Armstrong, "Big data: a revolution that will transform how we live, work, and think," *Inf. Commun. Soc.*, vol. 17, no. 10, pp. 1300–1302, 2014.
[7] O. F. AbdelWahab *et al.*, "Hiding data in images using steganography techniques with compression algorithms," *TELKOMNIKA*, vol. 17, no. 3, pp. 1168-1175, 2019.
[8] E. H. Rachmawanto *et al.*, "Imperceptible and secure image watermarking using DCT and random spread technique," *TELKOMNIKA*, vol. 17, no. 4, pp. 1750-1757, 2019.
[9] S. R. Maniyath and V. Thanikaiselvan, "A novel efficient multiple encryption algorithm for real time images," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1327-1336, 2020.
[10] J. Chen *et al.*, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340-353, 2018.
[11] Z. Hua *et al.*, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134-144, 2018.
[12] R. Afarin and S. Mozaffari, "Image encryption using genetic algorithm and binary patterns," *In 2013 10th International ISC Conference on Information Security and Cryptology (ISCISC), IEEE*, pp. 1-5, 2013
[13] A. Mahmood *et al.*, "An adaptive encryption based genetic algorithms for medical images," *In 2013 IEEE international workshop on machine learning for signal processing (MLSP), IEEE*, pp. 1-6, 2013
[14] M. George *et al.*, "Gold code generators in Virtex devices," *Xilinx Application Note xapp217*, vol. 1, no. 1, pp. 1-9, 2001.
[15] N. F. Standard, "Announcing the advanced encryption standard (AES)," *Federal Information Processing Standards Publication*, vol. 197, no. 1-51, pp. 3-3, 2001.
[16] P. FIPS, "46-\Data Encryption Standard," *Federal Information Processing Standards Publication, US Department of Commerce/National Bureau of Standards, National Technical Information Service*, vol. 46, 1977.
[17] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," *In International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg*, pp. 191-204, 1993.
[18] X. Wang and D. Xu, "Image encryption using genetic operators and intertwining logistic map," *Nonlinear Dynamics*, vol. 78, no. 4, pp. 2975-84, Dec 2014.
[19] W. K. Hastings, "Monte Carlo sampling methods using Markov chains and their applications," *Biometrika*, vol. 57 no. 1, pp. 97–109, 1970.
[20] I. S. Sam *et al.*, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995-2007, 2012.
[21] S. Das *et al.*, "Diffusion and encryption of digital image using genetic algorithm," *In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer, Cham*, pp. 729-736, 2015.
[22] M. R. Saranya *et al.*, "Algorithm for enhanced image security using DNA and genetic algorithm," *In 2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), IEEE*, pp. 1-5, 2015.
[23] G. Boeing, "Chaos theory and the logistic map," 2015, accessed 6 Sep 2019, https://geoffboeing.com/2015/03/chaos-theory-logistic-map/>.
[24] G. Xiao *et al.*, "New field of cryptography: DNA cryptography," *Chinese Science Bulletin*, vol. 51, no. 12, pp. 1413-1420, 2006.
[25] X. L. Chai *et al.*, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chinese Physics B*, vol. 25, no. 10, pp. 100503, Aug 2016.
[26] L. Ma *et al.*, "A four-wing hyper-chaotic attractor generated from a 4-D memristive system with a line equilibrium," *Nonlinear Dynamics*, vol. 81, no. 3, pp.1275-1288, 2015.

[27] M. Dridi *et al.,* "Cryptography of medical images based on a combination between chaotic and neural network," *IET Image Processing,* vol. 10, no. 11, pp. 830-9, 2016.
[28] M. Lin *et al.,* "Grayscale image encryption based on Latin square and Cellular Neural Network," *In 2016 Chinese Control and Decision Conference (CCDC), IEEE,* pp. 2787-2793, 2016.
[29] L. O. Chua and L. Yang, "Cellular neural networks: Theory," *IEEE Transactions on circuits and systems,* vol. 35, no. 10, pp. 1257-1272, 1988.
[30] N. B. Slimane *et al.,* "A Light Weight Method for Image Encryption Based on Chaos and Hope-field Neural Networks," *In Proceedings of Engineering Technology (PET),* pp. 417-422, 2016.
[31] M. Hénon, "A two-dimensional mapping with a strange attractor," *In the Theory of Chaotic Attractors, Springer, New York,* pp. 94-102, 1976.
[32] S. Sathasivam and W. A. T. W Abdullah, "Logic Learning in the Hopfield Networks," *Modern Applied Science,* vol. 2, no. 3, pp. 57-62, 2008.
[33] J. Wang, "Digital image encryption algorithm design based on genetic hyperchaos," *2016 International Journal of Optics,* 2016.
[34] Y. Liu *et al.,* "A family of new complex number chaotic maps-based image encryption algorithm," *Signal Processing: Image Communication,* vol. 28, no. 10, pp. 1548-59, 2013.
[35] G. Hu *et al.,* "Image Encryption Using Cellular Neural Network and Matrix Transformation," *In the Joint International Symposium on Artificial Intelligence and Natural Language Processing, Springer,* pp. 47-57, 2017.
[36] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimedia Tools and Applications,* vol. 76, no. 11, pp. 13681-701, 2017.
[37] K. Ratnavelu *et al.,* "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Processing,* vol. 140, pp. 87-96, 2017.
[38] T. Yang *et al.,* "Fuzzy cellular neural networks: applications," *In 1996 Fourth IEEE International Workshop on Cellular Neural Networks and their Applications Proceedings (CNNA-96), IEEE,* pp. 225-230, 1996.
[39] A. A. Abbasi *et al.,* "A Novel Image Encryption Model Based on Hybridization of Genetic Algorithm, Chaos Theory and Lattice Map," *Journal of Advances in Computer Research,* vol. 9, no. 4, pp. 129-44, 2018.
[40] S. Das *et al.,* "Image Encryption Based on Arnold Cat Map and GA Operator," *In Intelligent Engineering Informatics, Springer, Singapore,* pp. 19-28, 2018.
[41] V. I. Arnol'd and A. Avez, "Ergodic problems of classical mechanics," *New York, Benjamin,* 1968.
[42] S. Das *et al.,* "PSO-GA Hybrid Approach in Image Encryption," *In Annual Convention of the Computer Society of India, Springer, Singapore,* pp. 692-701, Jan 2018.
[43] M. Clerc, "Beyond standard particle swarm optimization," *In Innovations and Developments of Swarm Intelligence Applications, IGI Global,* pp. 1-19, 2012.
[44] D. Dey, "Image Encryption using Linear Cryptanalysis and different Fuzzy operations," *Image,* vol. 6, no. 4, pp. 1-8, 2018.
[45] M. Matsui, "Linear cryptanalysis method for DES cipher," *In Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg,* pp. 386-397, 1993.
[46] M. Kaur and V. Kumar, "Beta Chaotic Map Based Image Encryption Using Genetic Algorithm," *International Journal of Bifurcation and Chaos,* vol. 28, no. 11, pp. 1850132, 2018.
[47] R. Zahmoul and M. Zaied, "Toward new family beta maps for chaotic image encryption," *In 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC),* pp. 004052-004057, 2016.
[48] A. L. Da Cunha *et al.,* "The nonsubsampled contourlet transform: theory, design, and applications," *IEEE transactions on image processing,* vol. 15, no. 10, pp. 3089-3101, 2006.
[49] M. Kaur and V. Kumar, "Parallel non-dominated sorting genetic algorithm-II-based image encryption technique," *The Imaging Science Journal,* vol. 66, no. 8, pp. 453-62, 2018.
[50] G. Maddodi *et al.,* "A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding," *Multimedia Tools and Applications,* vol. 77, no. 19, pp. 24701-25, 2018.
[51] H. M. Mousa, "Chaotic genetic-fuzzy encryption technique," *International Journal of Computer Network and Information Security,* vol. 10, no. 4, pp. 10, 2018.
[52] S. Mozaffari, "Parallel image encryption with bitplane decomposition and genetic algorithm," *Multimedia Tools and Applications,* vol. 77, no. 19, pp. 25799-819, 2018.
[53] D. Dey and S. Paul, "Color Image Encryption using Single Layer Artificial Neural Network and Buffer Shuffling," *International Journal of Computer Sciences and Engineering,* vol. 7, no. 3, pp. 202-211, 2019.
[54] X. Y. Wang *et al.,* "A color image encryption algorithm based on Hopfield chaotic neural network," *Optics and Lasers in Engineering,* vol. 115, pp.107-118, 2019.
[55] T. Yoshida *et al.,* "Analytic study of chaos of the tent map: band structures, power spectra, and critical behaviors," *Journal of statistical physics,* vol. 31, no. 2, pp. 279–308, 1983.
[56] Y. Wu *et al.,* "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT),* vol. 1, no. 2, pp. 31-8, 2011.
[57] N. Ahmed *et al.,* "A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes," *International Journal of Computer Network & Information Security,* vol. 8, no. 12, pp. 18-29, 2016.
[58] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal,* vol. 27, no. 3, pp. 379-423, 1948.