International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Hybrid Imgae Encryption Based on Genetic Algorithm and Nueral Network

Areeg Abdallah Mokhatar Beram
Open University of Sudan
Computer Science department
Khartoum, Sudan

Dr. Ahmed Salah Al-Deen Abdallh
Open University of Sudan
Head Master of Computer Science Department
Khartoum, Sudan

***Abstract*— Biometric information and security, is the focusing zoon of worldwide. In Islamic countries such as kingdom of Saudi Arabia, female student facing a problem each time a security check and personal identification since the females covering their faces based on the religion and most of the students do not accept to put their photos into the entry and identification card of the university casing a problem identifying the student while the exams and while entering the university, this disadvantage increase the probability of using fake cards.**

In this paper a new solution is proposed to solve the problem of viewing student's photos, and encrypting the image using hybrid algorithm based on genetic algorithm and neural network, and the encrypted image is then inserted into 2D Barcode which called quick response code (QR-CODE). The image is acquired through

Keywords: Genetic Algorithm;Image Encryption; ANN; Artificial neural network.

INTRODUCTION

In today's world of growing technology security is of utmost concern. With the increase in cybercrime, providing only network security is not sufficient. Security provided to images like blue print of company projects, secret images of concern to the army or of company's interest, using image steganography and stitching is beneficial. As the text message is encrypted using AES algorithm and embedded in a part of the image the text message is difficult to find. More over since the secret image is broken down into parts and then sent to the receiver. This makes it difficult for the trespasers to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it becomes highly difficult for the intruder to detect and decode the document. There is no limitation on the image format that can be used right from Bmp to a GIF image can be used. It can be grey scale or colored images. The size of the message needs to be of only 140 characters.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. [2]

More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; [3] various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [4] are central to modern cryptography.

Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include military communications, electronic commerce, ATM cards, and computer passwords.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message (Alice) shared the decoding technique needed to recover the original information only with intended recipients (Bob), thereby precluding unwanted persons (Eve) from doing the same. The cryptography literature often uses Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.[5] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.

It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means.

These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

2.2 Literature Survey

1. New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture.

Jiun-In Guo and Jui-Cheng Yen [3] have presented an algorithm which was mirror like. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0. Then, the chaotic sequence is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

generated from the chaotic system. After that binary sequence is generated from chaotic system. And in last 4 stages image pixels are rearranged using swap function according to the binary sequence.

2. Lossless Image Compression and Encryption Using SCAN.
S.S. Maniccam and N.G. Bourbakis [4] have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

3. New Encryption Algorithm for Image Cryptosystems.
Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [6] used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used.

4. Technique for Image Encryption using Digital Signatures.
Aloka Sinha and Kehar Singh [4] have proposed a new technique in which the digital signature of the original image is added to the encoded version of the original image. A best suitable error code is followed to do encoding of the image, ex: Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after decryption of that image, the digital signature verifies the authenticity of the image.

5. Technique for Image Encryption using multi-level and image dividing technique.
Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha Wmn Lee, and SmJmng Kim[7] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures is regenerate to binary phase encoding and then these images are encrypt with binary random phase images by binary phase XOR operation.

6. Technique for Image Encryption using 1D chaotic map.
Fethi Belkhouche and Uvais Qidwai [8] used the method that can be used for binary images encryption with the possibility of using several keys ex: initial state, the external parameters and iterations' number.

7. A New Digital Image Scrambling Method Based on Fibonacci number.
They presented a method [09] for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in real-time situations. The scrambling effect is very sensible, the data of the image is re-distributed randomly across the whole image. The method can endure common image attacks, such as compression, noise and loss of data packet .They developed a method to study video scrambling and probe corresponding embedding algorithms for digital watermarks.

8. Technique for Image Encryption using chaos technique.
Guosheng Gu and Guoqiang Han [10] made a new highly optimized image algorithm using permutation and substitution methods. It was done in order to enhance the pseudorandom characteristics of chaotic sequences, an optimized treatment and a cross-sampling disposal is used
.

9. Technique for Image Encryption using chaos technique.
Huang-PeiXiao , Guo-ji Zang[11] made an algorithm using two chaotic systems . One chaotic system generates a chaotic sequence, which was changed into a binary stream using a threshold function. The other chaotic system was used to construct a permutation matrix. . Firstly, using the binary stream as a key stream, randomly the pixel values of the images was modified. Then, the modified image was encrypted again by permutation matrix.

10. Color Image Encryption Using Double Random Phase Encoding.
Shuqun Zhang and Mohammad A. Karim [12] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods.

11. Modified AES Based Algorithm for Image encryption.
M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R.Tourki [13] analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (W7,A5/1) to AES for ensuring the encryption performance.

12. Image Encryption Using Block-Based Transformation Algorithm.
Mohammad Ali Bani Younes and Aman [14] introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, and using the transformation algorithm it was rearranged, and then the
Blowfish algorithm is used for encrypting the transformed image their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

13. An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption.
Mohammad Ali Bani Younes and Aman Jantan [15] introduce a new permutation technique based on the combination of image permutation and a well-known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

14. Novel Image Encryption Algorithm Based on HashFunction.
Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [16] proposed an algorithm based on SHA-512 hash function, which was novel algorithm. It had two sections. Firstly does pre-processing operation to shuffle one half of image then hash function to generate a random number masks. The mask is then XOR with the other part of the image which is going to be encrypted.

15. Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps.
Ismail Amr Ismail, Mohammed Amin, and Hossam Diab [17] proposed chaos-based stream cipher, composing two chaotic logistic maps and external secret key for encryption of image. In this an external secret key of 104 bit and two chaotic logistic maps are used to differentiate between the encrypted image and the plain image. Further, the secret key is modified after encrypting of each pixel of the plain image which makes the encrypted image more robust. Then there is a feedback mechanism which increases the robustness of the proposed system.

16. New modified version of Advance Encryption Standard based algorithm for image encryption.
Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M.[18] presented a modification to the Advanced
Encryption Standard (MAES) to provide a high level security and better image encryption. The result shown by
them was higher than that of original AES encryption algorithm.

17. Image Encryption Using Affine Transform and XOR Operation.
Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [19] introduced a new algorithm using affine was two phase encryption decryption algorithm. Firstly using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys.
The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

18. Permutation based Image Encryption Technique.
Sesha Pallavi Indrakanti and P.S.Avadhani[20] introduced an algorithm on the basis of random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the process of encryption. The phase one was the image encryption. The phase two was the key generation phase. And the phase three was the identification process. This provide confidentiality to colour image with less computations.

19. Image Security via Genetic Algorithm.
Rasul Enayatifar and Abdul Hanan Abdullah [21] proposed a new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

20. Image Encryption Based on the General Approach for Multiple Chaotic Systems.
Qais H. Alsafasfeh and Aouda A. Arfoa[22] proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rossler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and highlevel security, high obscure level and high speed.

21. Statistical analysis of S-box in image encryption applications based on majority logic criterion.
Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal and Hasan Mahmood [23] propose a criterion to analyze the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption applications. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-poweraffine (APA), gray, Lui J, residue prime, S8 AES,
SKIPJACK, and Xyi Sboxes.

22. Image Encryption Using Differential Evolution Approach in Frequency Domain
Ibrahim S I Abuhaiba and Maaly A S Hassan [24] present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. In order to demonstrate the security of the new image encryption algorithm, key space analysis, statistical analysis, and key sensitivity analysis was carried out by them.

23. Image Encryption Based on Bit-plane Decomposition and Random Scrambling Qiudong
Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma [25] general random scrambling method was designed which has more

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

stable scrambling degree than the classical method Arnold transform. At first, they decomposed a gray image into several bit-plane images. Then we shuffled them by a random scrambling algorithm separately. Lastly, we merged the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image. Due to each bit-plane image is scrambled by using different scrambling random sequences, the bits located at the same coordinates in different bit-planes are almost not stay on the original positions when each bit-plane being scrambled separately. For each pixel, it's all bits of gray level, therefore, may be come from those pixels located different positions. Consequently, the reconstructed gray levels of image are changed ineluctable. It is obvious that our method can do both positions exchange scrambling and gray level change scrambling at the same time.

Genetic Algorithm

Genetic Algorithm has originated from the studies of cellular automata, conducted by John Holland and his colleagues at the University of Michigan [13].

A Genetic Algorithm is a searching technique used in computer science to find approximate solutions to optimization problems. GAs are a particular class of evolutionary algorithms that use techniques inspired by evolutionary biology such as inheritance, mutation, natural selection, and recombination (or crossover). Once we have the genetic representation and the fitness function defined, GA proceeds to initialize a population of solutions randomly, and then improve it through repetitive application of mutation, crossover, and selection operators. Researchers have adopted GA as a solution to optimization in various fields in recent years. GA as a solution to optimization problem started gaining popularity towards the end of the last century as used to solve optimization problems in construction. Its intrinsic parallelism facilitates the uses of distributed processing machines such as Distribution Network Planning [14]. Problems which appear to be particularly appropriate for solution by GA include Scheduling and State Assignment Problem. GA approach to Solve Map Color Problem has been experimented too.

Researchers have shown interest in GA approach to solve scheduling types of problems, like job shop scheduling problem [15]. It can be quite effective to combine GA with other optimization methods.

Hybrid GA approach is also being adopted to derive higher quality solutions in relatively shorter time for hard combinatorial real world optimization problems such as traveling salesman problem (TSP) [16]. Of late, researchers are also trying to explore the power of GA in various field of research like molecular research and genetic research to identify unknown genes of similar function from expression data [17].

4. THE PROPOSED ALGORITHM

The overall procedures for encrypting and decrypting an image are summarized as follows:

The steps of encrypting an image:

1. Loading an image.

2. Determining the height and width of image (H and W).

3. Checking the result of H mod 8 and W mod 8. If they are equal to 0 then go to

4th step otherwise doing H = H+ (8- (H mod 8)) and W = W+ (8- (W mod 8)).

4. Dividing the image into sets of block each block size's (8*8).

5. Considering a block B (w *h) where w and h are width and height of B.

5.1. Doing crossover operation.

Crossover proceeds in three simple steps:

5.1.1. Select randomly two strings from the block, one vertically another horizontally.

5.1.2. A random location from strings selected.

5.1.3. Swapped together the portions of strings on right side.

The secret key is used for crossover. In this research, secret key has two attributes termed a, b be/longing to 1 to 8. The crossover is done by swapping a to b in each vector.

5.2. Doing mutation operation for each vector Vi Do mutation by an another secret key of single variable of k. By the:

Vi[black]=255-vi[black]

5.3. Constructing an encrypted block from the set of N vector that is produced from the mutation

6. Getting the encrypted block

7. Repeating the 5th, 6th steps for all blocks.

8. Getting the encrypted image.

The steps of decrypting an image:

1. Loading an encrypted image

2. Getting the encrypted block

3. Doing mutation operation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

4. Doing crossover operation

5. Getting the decrypted block

6. Repeating 3ed and 4th steps for all blocks

7. Getting the decrypted image.

5. FEATURES

The proposed algorithm has been proved to provide high protection to the images data from illegal intrusions. It is fast in the process of encryption and decryption. The decryption process does not induce any loss of image data, and it has ability of dealing with different format of images, as will.

6. EXPERIMENTAL ANALYSIS

The proposed encryption algorithm can be classified as multiple criteria such as lossless, maximum distortion, maximum performance and maximum speed.

In this section, the proposed algorithm is applied on different sizes and types of images. The test images employed here show positive result.

Cryptography using genetic algorithm

Cryptography is used to change the original data in to unreadable format with the help of key. Greater complexity involved in the key generation process make it difficult for the cryptanalyst to attack the key. There are two types of cryptographic schemes based on the key used:

A. Symmetric Cryptography

Here same key is used for encryption and decryption. Symmetric key cryptography is one of the most important types of cryptography where key is shared between both the communicating parties. Symmetric key cryptography is used for private encryption of data to achieve high performance. For e.g. AES, IDEA, DES, etc.

B. Asymmetric Key Cryptography

Two different keys are used in Asymmetric cryptography where key for encryption is known as the public key, and the other for decryption, known as the private key. For e.g. RSA, Diffie - Hellman.

SECURITY OF KEY

In the literature review, it was observed that the characteristics feature that determine the strength of the key are not quantifiable but matrices might be used for evaluating and comparing cryptographic algorithm

.The characteristics that are considered are Type: Symmetric or Asymmetric; Functions: Integrity and authentication of message; Key size and rounds; and the complexity of the algorithm. The attacks that can be carried out to test the strength of the algorithm are brute force attack and differential cryptanalysis. The parameters used to judge the effect of these attacks are based on the key length and complexity of the algorithm from which key is generated. Key can be made complex by increasing the complexity involved in generation process. It will become very difficult for a cryptanalyst to attack the key. In this paper random number generator is used to generate key and genetic algorithm is used to make the key more complex. Which key should be selected will entirely depends on the fitness value of the different strings generated by random number.

A Random Number Generator (RNG)

A random number is a number generated such that it cannot be predicted, and which is difficult to reproduce sequentially and reliably.

Pseudo random number generators are used to generate a sequence of number that approximates the properties of random numbers.

Pseudorandom numbers are practiced for their speed in number generation. Random numbers are numbers that occur in a sequence such that two conditions are met:

(1) The distribution of values are uniform across a defined set interval or, and

(2) Prediction of future values on the basis of past or present ones is impossible.

Genetic Algorithm

Genetic algorithm [5] is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic algorithms contain: selection, crossover and mutation.

The GA goes through the following cycle: Selection, crossover, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

A. Selection

It is quantitative approach where the chromosomes from populations are chosen to reproduce based on fitness value of chromosomes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

B. Crossover

In crossover operation two chromosomes are taken and a new is generated by taking some features of first Chromosome and the rest over from another or second chromosome. For example, the strings 11110010 and 01001111 could be crossed over after the third locus in each to produce the two offspring 11110111 and 01001010. There are three type of crossover operation Single Point Crossover, Two Point Crossover, Uniform Crossover. Figure 2 showed the working of crossover operator. Fig (a) illustrates the bits contained in two strings. Fig (b) both the strings are detached from their third locus. Fig (c) new population after crossover operation.

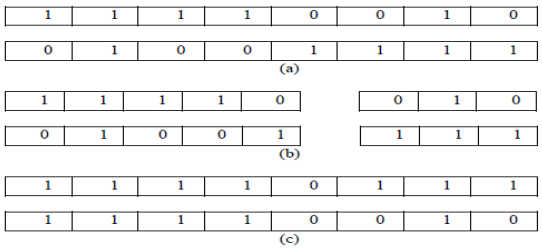

Fig 1. Working of Crossover Operator

C. Mutation

Mutation is used to maintain genetic diversity from one generation to the next generation of population.

It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in a string of bits Gas. These operators randomly interchange two bits or simply flip the bit in a chromosome. For example, the string 00000111 might be mutated in its fifth position to yield 00001111. The basic GA Cycle has been showed in fig1.

Fig 2. Basic Model of Genetic Algorithm

In the above figure the process starts with initial population. From the initial population the individuals which in having maximum fitness value are selected for the further process. Fitness value is calculated from the fitness function. The selected population is the mated using cross over operation and mutated to generate new best individuals.

Advance Encryption Standard

AES is a symmetric block cipher. It means that it uses the same key or a single key for both encryption and decryption.

The algorithm is based on Rijndael principle which allows a variety of block and key sizes. The block and key can be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm.

The four stages are as follows:

1. Substitute bytes

2. Shift rows

3. Mix Columns

4. Add Round Key

The tenth round simply eliminates the Mix Columns step.

The generation of initial population of chromosomes is in hexadecimal number using random function. This initial population is 128 bit long. Here ‘n’ number of population is generated. All this individuals are sent to a fitness function. This fitness function is a maxima function which means that the individual which is having maximum fitness value is selected for the further process. After this process we select two best individuals. On the selected individuals one point crossover is performed and the point of crossover is decided on the basis of a random number. After performing crossover we get the offspring of the selected individuals. Now again fitness function is applied on the children and if their fitness value is better than the parent, then parents are replaced by the children otherwise not. Now the output of previous step will work as input of mutation operation. After mutation we will get the final key which will be used for encryption process. The key generation process from the Genetic Population has the following steps:

A. Initial Population Generation:

128 bit long initial populations of chromosomes are generated using a random number generator in decimal number.

B. Conversion:

The decimal number is converted in to hexadecimal number.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

C. Fitness Calculation:

The fitness value of each individual is calculated. The fitness value is calculated on the basis of symbol which is repeated maximum. The fitness function can be expressed as:

$F = n + (€ /m)$

Where

F = Fitness Function.

n = Total number of symbols used in key formation.

m = Percentage of maximum appeared symbol.

€ = Ideal Percentage of each symbol.

D. Crossover:

On the randomly selected two chromosomes one point cross over is performed on the basis of a random value.

After crossover operation we get two new offspring's generated from their parent chromosome.

E. Fitness Check:

Now again the fitness checking is done on the new child chromosome and if they are found better than the previous one are replaced by their child otherwise not.

F. Mutation:

Now mutation is performed on a randomly selected chromosome and its new fitness value is calculated.

G. Fitness Check

Again Fitness value of whole population of that particular run is checked and maximum one is taken in to account. The whole process is performed hundreds of time. In each iteration population having maximum fitness value is recorded. After the stopping condition is met the population with maximum fitness value is selected as a key for encryption. Figure 3 illustrate the key Generation Process.

For encryption, Advanced Encryption Standard (AES) has been used. Symmetric key algorithm is proposed due to its computation speed and less overhead in key management.

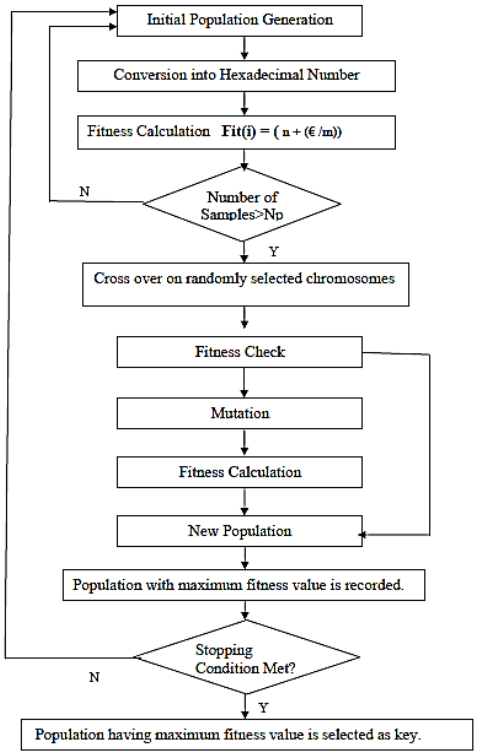

Fig 3. Key Generation Process Using Genetic Algorithm

REFERENCES

[1] John Justin M, Manimurugan S , "A Surve on Various Encryption Techniques ", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[2] Ephin M, Judy Ann Joy and N. A. Vasanthi, " Survey of Chaos based Image Encryption and Decryption Techniques " , Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA).

[3] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.

[4] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34,1229-1245,2001.

[6] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", The Journal of Systems and Software 58 , 83-91,2001.

[7] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003

[8] Fethi Belkhouche and Uvais Qidwai , "Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.

[9] Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number,"Proceeding of the IEEE Inter Symposium On Circuits and Systems,Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

[10] Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems", IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.
[11] Guosheng Gu ,Guoqiang Han, "An Enhanced Chaos Based Image Encryption Algorithm", IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.
[12] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.
[13] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27, 2007.
[14] Wang Ying, Zheng DeLing, Ju Lei, et al., "The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004
[15] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.8, April 2008.
[16] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function", 6th Iranian Conference on Machine Vision and Image Processing, 2010.
[17] Ismail Amr Ismail, Mohammed Amin, Hossam Diab ,"A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.
[18] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M., "A new modified version of Advance Encryption Standard based algorithm for image encryption",Electronics and Information Engineering (ICEIE), 2010 International Conference .
[19] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation ",International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).
[20] Sesha Pallavi Indrakanti,P.S.Avadhani, "Permutation based ImageEncryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28 ,No.8, 2011.
[21] Rasul Enayatifar , Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.
[22] Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.
[23] Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion", International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011.
[24] Ibrahim S I Abuhaiba , Maaly A S Hassan, "Image Encryption Using Differential Evolution Approach In Frequency Domain" , Signal & Image Processing an International Journal (SIPIJ) Vol.2, No.1, March 2011.
[25] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University , vol. 09 IEEE, 2012.