I. J. Computer Network and Information Security, **2018, 3, 60-66**
Published Online March 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.03.07

Image Cryptography with Matrix Array Symmetric Key using Chaos based Approach

Tarun Kumar
Department of Computer Science Engineering Radha Govind Group of Institutions, Meerut UP (India)
E-mail: taruncdac@gmail.com

Shikha Chauhan
Department of Computer Science Engineering Radha Govind Group of Institutions, Meerut UP (India)
E-mail: cshikha1590@gmail.com

Received: 27 September 2017; Accepted: 13 December 2017; Published: 08 March 2018

***Abstract*—**With the increase in use of digital technology, use of data items in the format of text, image and videos are also increases. To securely send this data, many users and smart applications have adapted the image encryption approach. But the existing concepts are based on general AES approach. There is need to securely send the data with the addition of some expert image encryption and key generation approach. In this paper, we are using Matrix Array Symmetric Key (MASK) for the key generation and Chaos based approach for the image encryption. The main function of MASK is to generate the key for the encryption and decryption. The encryption process involves the generation of key. We have considered the key of MASK-256 for the encryption having 16 rounds. Chaos based concept has been considered for the encryption of image. Here, permutation- substitution based chaos based approach has been adopted for the image encryption. Moreover, in this approach, we have adapted the concept of partial encryption of image pixels instead of complete encryption so that in case of arrack, intruder can be confused with the partial encrypted image. In this approach, different image samples having different sizes have been considered. Further, concept is evaluated based on the parameters of Information Entropy, Elapsed Time, Precision, Recall and F-Measure.

***Index Terms*—**Matrix Array Symmetric Key, Chaos based Encryption, Cryptography, Image Security, and Image Encryption.

I. INTRODUCTION

Digital image is the most commonly used format of content to share some information with anyone. But to securely send this format, there is need of some cryptography approach. Cryptography is a technique used to avoid unauthorized access of data [1]. It has two main components; a) Encryption algorithm, and b) Key [2]. Sometime, multiple keys can also be used for encryption. A number of cryptographic algorithms are available in market such as DES, AES, TDES and RSA. The strength of these encryption algorithms depends upon their key strength. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and reduce the overheads of the system. The long key length takes more computing time to crack the code and it becomes difficult for the hacker to detect the cryptographic model. Cryptography is basically divided into two categories; a) Symmetric Cryptography [3], and b) Asymmetric Cryptography [4]. In symmetric cryptography the key used to encrypt the message is the same as the key decrypting the message whereas in asymmetric cryptography different key is used for encryption and decryption. Asymmetric algorithms are relatively slower than symmetric algorithms but provide a good security level. So, for the successful transaction of the image data, we are considering the MASK approach along with Chaos based Encryption algorithm.

Further, structure of the paper has been discussed here. Section II presents the existing work related to image encryption, Section III brief about the basic concepts of MASK approach and Chaos based Encryption concept, Section IV presets the proposed algorithm used for image encryption, key generation and image decryption, Section V discusses about the result and comparison of the proposed concept with other concepts. Section VI concludes the paper.

II. RELATED WORK

Roy et al. [5] have proposed a colour image encryption system based on the hyperchaos permutation system. The authors have also studies the process of encryption and decryption based on the concept of Vertical-cavity Surface-emitting Laser (VCSEL). The two nearly synchronized VCSEL's are investigated named as master VCSEL and slave VCSEL. The two VCSEL systems operate in a chaotic manner and lowering the value of coupling coefficient also lowers the correlation value between the two lasers. The lasers become unsynchronised when the coupling value is increased beyond the optimum value. In the proposed system, a

RGB based image is considered and using the master laser key vector is generated. Then the pixel values of the image are permuted. After the pixel permutation, bit level permutation is done and after operating Bit XOR corresponding cipher image is obtained. The proposed system is simpler and faster as compared to other chaos based systems.

Chai et al. [6] have proposed DNA operations and chaotic system based encryption algorithm. The plain text to the algorithm is in image form and then it is encrypted and corresponding cipher image is generated. Initially a 256 bits key is generated using the secure hash algorithm SHA 256. The encryption process involves permutation and diffusion procedures. Matrix P is generated based on plain image .A wave based permutation scheme is used at DNA level to generate the DNA matix P2 and confused matrix P3 is generated by permuting the P2. After the permutation, row wise image diffusion is performed and results into P4 matrix. The diffused DNA matrix is fused by a key matrix generated from 2D chaotic system. In order to modify the image initial values and system values, hamming distance is calculated. The proposed algorithm is secure and highly reliable and has shown resistance to the known-pain text and chosen-plain text attacks.

Wang [7] has proposed an image based encryption algorithm. The encryption algorithm is based on the concepts of chaotic theory. The encryption parameters obtained from the chaotic system are further optimized with the help of Genetic algorithm in order to get the best encryption parameters. The concept of Genetic Hyperchaos system uses the features of both genetic algorithm and chaos system. Initial population is generated by considering enough number of the chaotic sequences. A pixel matix P is generated with the scrambled pixel values. The generated matix is divided into two parts and from the matix generated through numerous iterations the different matrix operations are replaced. In this way pixel diffusion is performed. In the next step, genetic algorithm is used to improve the population diversity. The procedure is continued until the best fitness function is obtained. Statistical analysis, key analysis etc. are done to analyse the performance of the system.

Li [8] has presented the performance analysis of the Hierarchical Chaotic Image Encryption (HCIE) algorithm. The author has analysed the algorithm by performing cipher text-only attacks and known-plain text attacks. HCIE is an image encryption algorithm based on the two stages of permutation. The first level is high level which permutes the plain text image by dividing into different blocks. The second level is low level which permutes the pixel values of each image block. The author has observed that the HCIS algorithm is over-estimated. The algorithm is only permutation based algorithm and it is not sufficient and also it is less secure than the permutation algorithms without hierarchical structures. The author has suggested that for better and more secure encryption the algorithm should make combine use of the concept of permutation and substitution.

Zhao et al. [9] have proposed a chaos based image encryption system. The proposed system uses the chaotic concept of Arnold maps. The proposed system is based on the permutation and substitution procedures. Instead of many iterative rounds, only one round of permutation and substitution is performed. Also, in order to increase the speed of encryption process, the process of permutation and substitution is considered row wise and column wise rather than pixel by pixel. Initial stage is permutation stage; the image here is in form of a 3-D matrix. With the help of Arnold map, the pseudo-random vectors for permutation are generated. In the second step, two more pseudo-random vectors are generated for the substitution process. The 3-D matrix is transformed to 2-D matrix for the process of permutation. The 2-D matix is then substituted row and column wise. The matrix is then again transformed to 3-D marix and then converted to the coloured image. The image thus obtained is cipher image. In order to analyse the performance of the proposed algorithm, key space analysis, histogram analysis, sensitivity analysis etc. are done. The proposed algorithm has shown effective results and is secure in nature.

Paul and Nair [10] have presented the 2-D array (Matrix) based procedures for the encryption of the image data. The matix based procedures considered are substitution and diffusion. The image is encrypted using the block cipher technique with 16 rounds of substitution and diffusion. The size of the block is 128 bits and referred as P whereas key is referred as K having size of 128 bits as well. Initially, matrix M is generated using the key K and two different matrices for the round operations are generated from the sub-keys. The block of data i.e. P is iterated through the 16 rounds and corresponding cipher text is generated. The proposed matrix based encryption algorithm is tested on different images with different size and the obtained results are then compared to the results obtained from Advanced Encryption Standard (AES) algorithm. The test results obtained show that the proposed algorithm is eight fold times faster than the AES algorithm.

Dipanwita Debnath [16] proposed a new steganography method for spatial domain including new mapping technique for the transmission of secret messages. The algorithm is a combination of message encryption and message hiding into the cover image thus providing better security. The algorithm has the capability to convert any message to text using bit manipulation tables. After that hill cipher technics is applied to the text message and the message is hidden into red, green and blue colors of a particular selected image. The algorithm has been tested and compared with MSE, PSNR, SC, AD, MD and NAE by demonstrating histogram and stegano image.

Dadhich and Yadav[18] also studied the strong cryptography and computational intelligence requirements. Focus is laid on improved cryptographic algorithms in the field of optimization. The review domain includes integrated genetic algorithms, immune

computing, crossover and mutation operators and fuzzy for optimization of candidate objects. These techniques have improved the fitness levels of candidate groups. At the last, these cryptographic techniques without computational intelligence are also compared with the former techniques with computational intelligence.

Khalil [20] have advised a new symmetric-based encryption/decryption approach for securing audio signal to guarantee end-to-end secrecy for speech in real time communication systems. The performance of the suggested approach is compared with that acquired when applying the well-known Asymmetric RSA technique. It processes the transmitted audio signal encrypting each acquired sample and decrypting it at the receiver. The technique can be applied uniformly to both digital and analog audio signals such as VoIP, GSM, analogue Radio, Telephone.

Dawood [21] suggested a new iterated symmetric cipher, which is designed with Substitution and Permutation Network (SPN) structure and depends on strong mathematical built. It uses a algorithm for encryption /decryption processes, which consists of four main stages that roughly similar in its work to the Advance Encryption Standard (AES) stages. Starting by the Round key addition, Reversible Mix columns operation, Reversible Shift rows operation and Sub Byte operation.

III. Basic Concepts

This section presents the basic concepts of Matrix Array Symmetric Key (MASK) and Chaos based Encryption approach.

A. Matrix Array Symmetric Key (MASK)

The Matrix Array Symmetric key (MASK) [11] is a symmetric key encryption algorithm which makes use of one matrix and four arrays during the encryption process. The input or plain text to the algorithm is 128 bit data block and corresponding 128 bit cipher text is generated by the algorithm. The size of the secret key is also 128 bits. The algorithm works on the concept of substitution and diffusion. MASK works in three steps. First step involves the initialization of the matrix from the plain text. The matrix is used by the key schedule algorithm in order to generate the sub keys for the diffuse operations. Also the matrix is referred during the process of substitution and diffusion, to substitute the matrix's value of selected row. The second step in MASK is Key Scheduling. Here 16 different pairs of sub keys are generated for the 16 different rounds of diffusion. The third and final step is Substitution and Diffusion. The output of this step cipher text in the form of 16 bytes block data. Fig 1 shows the block diagram of encryption process in MASK.

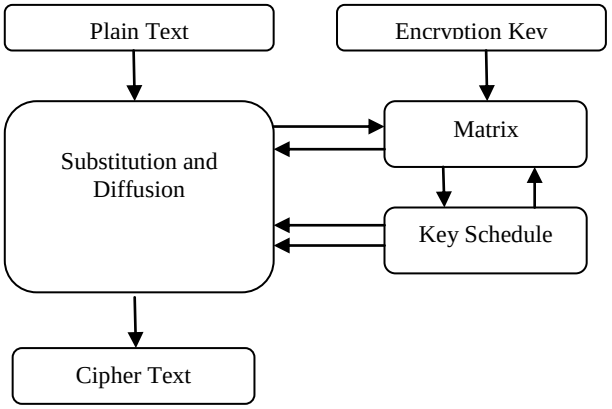

Fig.1. Block diagram of Encryption process in MASK

B. Chaos based Image Encryption

There are many encryption algorithms for the encryption of text and image data. The computation time for the encryption of image data in case of traditional algorithms is very high. In case of large amount of bulk data, these algorithms are not much reliable and exhibits low level efficiency. In order to remove the limitation of the traditional encryption algorithms, a new concept known as Chaos Based Image Encryption was introduced.

The Chaos Based Encryption techniques are the one of the most efficient and reliable techniques. Also they are efficient in dealing with heavy multimedia data and offers great security and reliability [12]. The chaos based systems deals only with real numbers thus making them different from the other cryptography algorithms which deal with finite sets. The main concept of chaotic system deals with the process of synchronization and controlling between the other two chaotic systems. This concept is referred as Chaotic Dynamical System [13]. In order to synchronize chaotic system numerous techniques are there like, shift key, use of chaotic maps, chaotic masking etc. The high sensitivity to its initial condition, the ergodicity, parameter value etc. makes the chaotic systems rich in implication as compared to the other cryptosystems. In Chaos based encryption, there is the availability of lot of concepts. In this research work, we have considered pixel wise permutation-substitution approach [14] for the image encryption.

IV. Proposed Concept

In this section, the proposed algorithm of MASK with Chaos based encryption is presented. The main function of MASK is to generate the key for the encryption and decryption. The encryption process involves the generation of key. Chaos based concept has been considered for the encryption of image. Here, permutation- substitution based chaos based approach has been adopted for the image encryption. Moreover, in this approach, we have adapted the concept of partial encryption of image pixels instead of complete encryption so that in case of arrack, intruder can be confused with the partial encrypted image. This proposed algorithm is structured as below:

ALGORITHM (IMAGE ENCRYPTION)

Initialization

Step 1: First the image is divided to blocks and they pass through bit plane coding. Alternate bit planes are complemented amongst adjacent pixels XOR'ed to reduce the correlation of the cipher image.

Step 2: In each block select three pixels (size 3×8 = 24 bits), which are combined and split into four pixel values (4×6 = 24bits) resulting in extra no. of column's, will change the image size making it difficult to identify the original image.

Step 3: Alternate columns are shifted left by two bits, when combined in to four values each pixel will be a 6 bit data, i.e. '00' followed by 6 bits of data.

Step 4: This is followed by the primitive encryption algorithm and it is iterated for maximum number of iteration rounds.

Image Encryption Algorithm

Step 1: Covert 2D image into 1D array and then performs the pixels wise scanning.

Step 2: Consider a block size of 8 × 8 and convert them in to binary values.

Step 3: Consider a Secrete key using MASK approach as discussed in the key "Generation Section". From the initial conditions the chaotic maps are allowed to iterate through various orbits. Then, based on the chaotic system, binary sequence is generated to control the bit-circulation functions to perform the successive data transformation on the input data.

Step 4: Convert the chaotic sub key in to binary bit values.

Step 5: Each 8 × 8 sub block of image pixel values circularly shifted by chaos sequence generated from maps.

Step 6: Perform the encryption by the chaotic sequence key values, which is obtained from the orbits of chaos maps iteration.

Step 7: Initialize the encryption process and start the iteration process with the sequence of real numbers.

Step 8: Arrange the chaotic sequence in descending order to get the sorted sequence.

Step 9: Permute the pixels of the cipher image with permuting address code and replace the row pixel with the row pixel for from 1 to n.

Step 10: Repeat the process till the maximum number of iteration reached and get the encrypted image into 1D form.

Step 11: Transform the 1Dimension image 2Dimentions.

ALGORITHM (KEY GENERATION)

Step 1: Generate the MASK-256 key for the image encryption process with four stages of (i) Substitute Bytes (ii) Shift rows (iii) Mix columns (iv) Add round key.

Step 2: Consider the image pixels and begin the process of key generation by using the MASK process having *C(i)* is the bit wise image pixels and matrix *Md* for the 16 rounds and 256 blocks.

2.1. Let $i = 1$.

2.2. Search and locate the byte value represented by $C(i)$ in the ith row of the matrix *Md*.

2.3. Obtain the column number j, in the ith row where the byte $C(i)$ has been located.

2.4. Assign value $(j\text{-}1)$ to $P(i)$ which gives inverse substitution to $C(i)$.

2.5. Increment i.

2.6. Go to step 1 till i becomes > 16 (the block size is 16).

Step 3: Insert the generated key during the beginning of the process.

ALGORITHM (IMAGE DECRYPTION)

Step 1: During Decryption, Receiver needs to enter the same key that was used by sender during the encryption process.

If key match found,

Then, apply chaotic permutation-substitution in the reverse to get the pixels at their original position.

Else

System will be interrupted and encrypted image will not be received.

Step 2: Obtain the output decrypted image.

V. RESULT & COMPARISON

The proposed algorithm is implemented with Graphical User Interface in MATLAB simulation tool. The system is considered in two parts of Encryption and Decryption. During encryption process, a unique key have been used for the encryption of image. Here, partial image encryption concept has been considered so that intruder cannot interrupt the system. During decryption, there should be availability of same key at receiver end to decrypt the image and obtain the original image. Fig 2 and Fig 3 shows some of the examples of decrypted images that have been considered during the experimentation. Here histograms of images have also been shown in the figures.

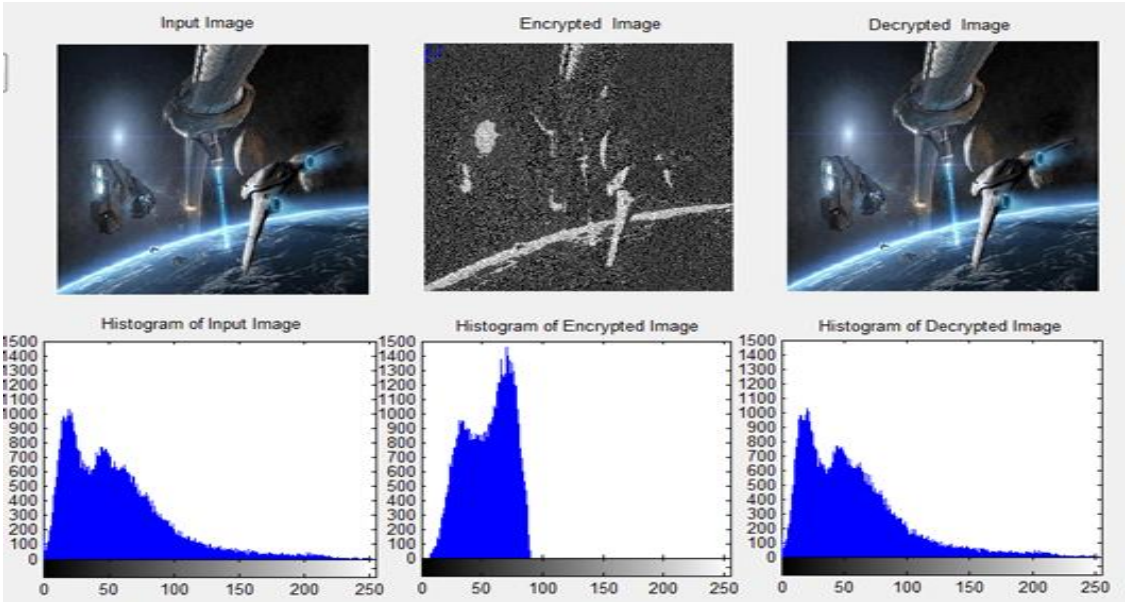

Fig.2. Encrypted, Original and Decrypted Image Sample 1 along with their Histograms

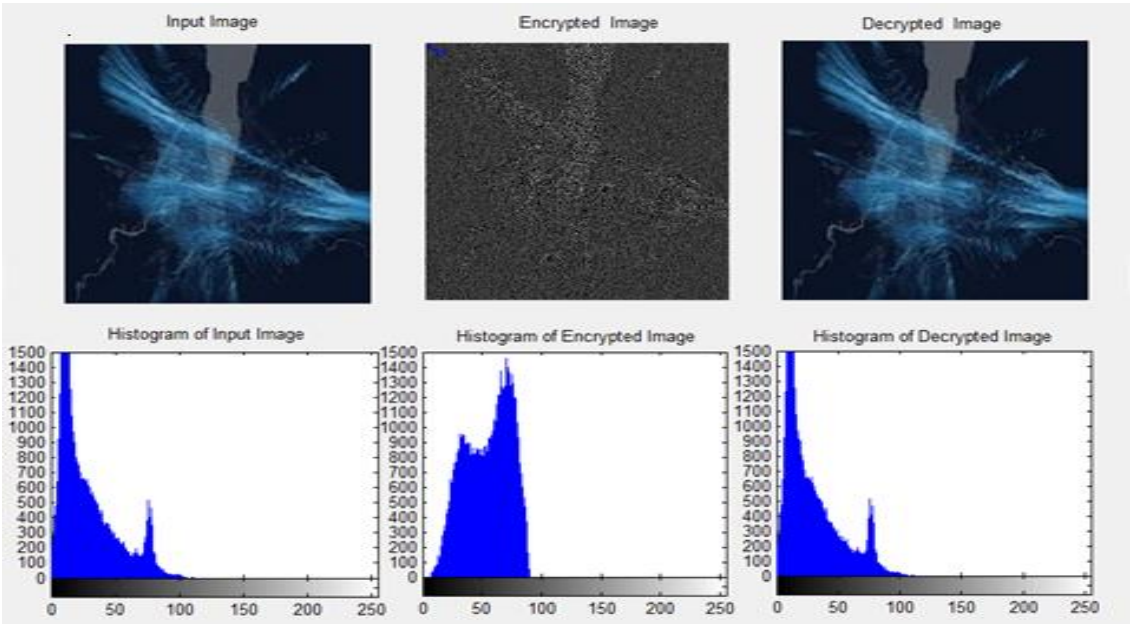

Fig.3. Encrypted, Original and Decrypted Image Sample 2 along with their Histograms

We have performed the above experimentation for different type of images and evaluated the encryption time and decryption time for these images as per their size. This evaluated time is elapsed time and shown in table 1. Elapsed time is the term used for time taken for the image processing during various operations. Here, elapsed time is considered to define the time taken for the image to encrypt and decrypt using MASK key. The value of the elapsed time may vary for the process of encryption and decryption because during encryption, the key have to set their values to encrypt, but decryption just performs the reverse process of encryption.

Table 1. Evaluated Values on Elapsed Time

Image size (Pixels)	Image size on disk	Encryption time	Decryption time
128*128 (image 1)	6.87 KB	2.46293	0.430659
128*128 (image 2)	8.82 KB	2.52614	0.362565
256*256 (image 3)	27.7 KB	2.28798	0.587776
256*256 (image 4)	39.6 KB	2.1137	0.648175
256*256 (image 5)	40.1 KB	2.3917	0.447809
512*512 (image 6)	66.7 KB	2.52776	0.378995
512*512 (image 7)	133 KB	2.13712	0.462269

Further, parameter of Information Entropy has been considered which is used to compare the proposed technique with the other concepts of AES and MAES. Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [15]. Modern information theory is concerned with error- correction, data compression, cryptography, communications systems, and related topics. After evaluating Information entropy, we obtain its entropy = 8, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. The evaluated results for the considered concepts are shown in table 2.

Table 2. Comparison based on Information Entropy

Parameters/Algorithms	Information Entropy
AES	7.9979
MAES	7.9982
Proposed Concept	7.9995

From the above comparison table 2, we can say that proposed algorithm gives better results as compare to other AES and modified AES algorithm. The comparison values of Information Entropy are also shown in fig 4.

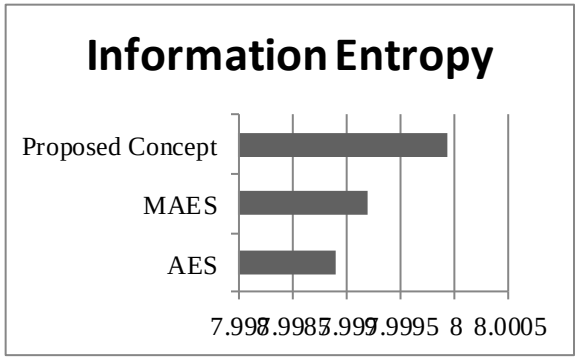

Fig.4. Comparison based on Information Entropy

Also the parameters of Precision, Recall and F-measure have been calculated. Precision denotes the probability that encrypted pixels from the image that are truly detected while decryption. Recall shows the probability that the encrypted pixels which are actually detected. F-measure is the combination between recall and precision. The Precision and Recall are further used to calculate the value of F- measure. The evaluated values of Precision, Recall and F-measure are shown in table 3 and fig 5.

Table 3. Evaluated Values of Precision, Recall and F-Measure

Evaluation Terms	Evaluated Values
Precision	91.6667
Recall	78.5714
F-Measure	84.6154

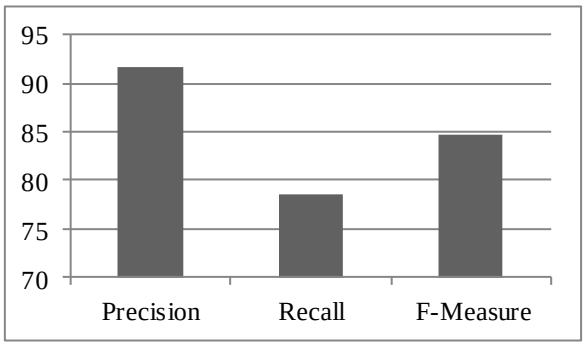

Fig.5. Evaluated Values of Precision, Recall and F-Measure

VI. Conclusion

The aim of the cryptography is to securely send the data whether it would be images or other forma of data. In this research work, we have considered the imagery based data. Study of various encryption algorithms has been successfully done. From the existing algorithms, it can be seems that the strength of the algorithm depends on the strength of the key. In this concept, we have implemented the proposed algorithm on different types of images. Parameters have been evaluated in terms of elapsed time, information entropy, precision, recall and f-measure. From the comparison results based on the Information entropy, it can be seems that MASK key generation approach is better as compare to AES and MAES (fig 4). Also the parameters of precision, recall and f-measure have been evaluated to check the correctness of concept.

References

[1] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. Handbook of applied cryptography, CRC press 1996.

[2] Stallings, W. Cryptography and network security: principles and practices. Pearson Education India 2006.

[3] Stark, E., Hamburg, M., & Boneh, D., "Symmetric cryptography in javascript", Computer Security Applications Conference, 2009. ACSAC'09. Annual (pp. 373-381). IEEE.

[4] Ganesan, R..U.S. Patent No. 5,737,419. Washington, DC: U.S. Patent and Trademark Office 1998.

[5] Roy, A., Misra, A. P., & Banerjee, S. "Chaos-based image encryption using vertical-cavity surface-emitting lasers", arXiv preprint arXiv: 1705.00975 2017.

[6] Chai, X., Chen, Y., & Broyde, L. "A novel chaos-based image encryption algorithm using DNA sequence operations", Optics and Lasers in Engineering, 88, 197-213 2017.

[7] Wang, J. "Digital Image Encryption Algorithm Design

Based on Genetic Hyperchaos", International Journal of Optics, 2016.
[8] Li, C. "Cracking a hierarchical chaotic image encryption algorithm based on permutation", Signal Processing, 118, 203-210 2016.
[9] Zhao, J., Guo, W., & Ye, R. "Achaos-based image encryption scheme using permutation-substitution architecture", Int. J. Comput. Trends Technol, 15(4), 174-185 2014.
[10] Paul, A. J., & Nair, L. R. "Matrix based Substitution and Diffusion Procedure for Fast Image Encryption", International Journal of Computer Applications, 80(3) 2013.
[11] Paul, V., & Mythili, P. (2007). "Matrix Array Symmetric-Key Encryption". Journal of the CSI Vol, 37(1) 2007.
[12] Usama, M., Khan, M. K., Alghathbar, K., & Lee, C. "Chaos-based secure satellite imagery cryptosystem". Computers & Mathematics with Applications, 60(2), 326-337 2010.
[13] Belazi, A., El-Latif, A. A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms." Optics and Lasers in Engineering, 88, 37-50 2017.
[14] Belazi, A., Khan, M., El-Latif, A., & Belghith, S. "Efficient cryptosystem approaches: S-boxes and permutation substitution based encryption", Nonlinear Dynamics, 87(1), 337-361 2017.
[15] Shannon, C. E. "Communication theory of secrecy systems", Bell system technical journal, 28(4), 656-715 1949.
[16] Debnath, D., Deb, S., & Kar, N. "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher & RGB Image Steganography" In Computational Intelligence and Networks (CINE), International Conference on (pp. 178-183). IEEE 2015.
[17] Avasare, M., & Kelkar, V. "Image Encryption using Chaos Theory", International Journal of Global Technology Initiatives, 3(1), B135-B142 2104.
[18] Dadhich, A., & Yadav, S. K. "Evolutionary Algorithms, Fuzzy Logic and Artificial Immune Systems applied to Cryptography and Cryptanalysis: State-of-the-art review", optimization, 3(6) 2014.
[19] M.I.Khalil, "Real-Time Encryption/Decryption of Audio Signal", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.2, pp.25-31, 2016.DOI: 10.5815/ijcnis.2016.02.03
[20] M.I.Khalil, "Real-Time Encryption/Decryption of Audio Signal", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.2, pp.25-31, 2016.DOI: 10.5815/ijcnis.2016.02.03
[21] Omar A. Dawood, Abdul Monem S. Rahma, Abdul Mohssen J. Abdul Hossen, "New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.4, pp. 29-36, 2017.DOI: 10.5815/ijcnis.2017.04.04

Authors' Profiles

Tarun Kumar is an Associate Professor in Radha Govind Group of Institutions, Meerut(U.P.) ,India.He has completed PhD in Computer Science Engg in 2012 from Bansathali University, Bansthali (Raj.). He has also completed M.Tech in Information Technology in 2006 from GGSIP University Delhi. He has two years of industrial experience and 12 years of teaching experience. His research interests include Optimization Techniques, Soft computing technologies, Wireless Security and Image Processing. His research papers are published in various national and international conferences and intentional journals.

Shikha Chauhan, BTech in Computer Science Engg. From Dr. A.P.J. Abdul Kalam Technical University. Lucknow, Uttar Pradesh India .Currently pursuing MTech in Computer Science Engg. from Radha Govind Group of institutions, Meerut India Uttar Pradesh. her current research interests include: cryptography, Image Processing.

How to cite this paper: Tarun Kumar, Shikha Chauhan,"Image Cryptography with Matrix Array Symmetric Key using Chaos based Approach", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.3, pp.60-66, 2018.DOI: 10.5815/ijcnis.2018.03.07