A Framework for Digital Image Encryption using Chaotic Baker Map with SHA Algorithm

S Saravanan, M Sivabalakrishnan

Abstract*: Recently, security for the image is becoming very important. Image Encryption is the only choice in protecting the digital image by transforming the image into an unreadable format. There are many methods used to protect against unauthorized access. This research proposes a framework for image encryption using Chaos Baker map with SHA-1 algorithm. The Chaotic Baker map is a randomization technique used to make the pixels more shuffled. Key generation is essential part of image encryption, which will be carried out by SHA-1 algorithm. Experimental results show that the proposed method is well suited for high security, key sensitivity and resists various attacks.

Keywords: Chaotic map, Image encryption, Key Generation, SHA.

I. INTRODUCTION

In the last few years, the internet and multimedia have been improved rapidly; increasingly multimedia data seem in our day-to-day lives like image, audio, and video. But still digital image is the most commonly used multimedia data in the communication. However, Internet brings us fantastic comfort in addition to a few terrible results including non-public secrecy revelation and military secrets and techniques leakage. Therefore, image encryption has received substantial interest and studies.

In order to provide security to the image pixel by inhibiting illegal access, image encryption is considered to be a highly effective and famous method for stabilizing multimedia data. The chaotic map may be accustomed generate a series of pseudo-random numbers by continuance instinctively in step with the initial parameters. The chaos-based cryptography methodology is assumed to be terribly appropriate for image cryptography, like the distinctive characteristics of the chaotic map. Chaotic map is highly subtle to its early sets and control constraints. There are several chaos-based image cryptography schemes are extensively considered.

Though, these chaos based schemes have not been resistant by the presence of vulnerabilities through certain attack techniques like Cipher-plaintext attack and selected encryption attack. Cryptanalysis aimed at demolishing an existing crypto system to test security and improve the original schema. Zhang's coding scheme based on three-dimensional bit matrix permutations was corrupted by encrypting a symmetric image coding scheme.

A new image coding scheme that uses an additional substitution structure has also coded and successfully attached color image coding based on the hyper-chaotic hybrid system. If it can survive several attacks then cryptographic system is considered to be safe. The rest of the work is systematized as follows. Section 2 confers literature review. Section 3 illustrates the proposed system of this paper. In section 4, we have demonstrated the experimental results to improve high security using Chaotic Baker map with SHA-1 algorithm.

II. LITERATURE SURVEY

Akshay Chopra et al [8], introduced Rozouvan's expanded version of image encryption algorithm, which incorporates fractal image features as key and theory of chaos. The usage of chaotic system in Rozouvan's algorithms help to strengthens the algorithm and be responsible for a high level of security. Improved algorithms improve robust performance, as well as inheriting the characteristics of the original algorithm. Map of Arnold cats based on permutation guarantees an almost zero relationship between the adjacent pixels of the scrambled image and the image of the encryption process makes dependent on key features. The main limitation in Rozouvan was that the fractal key image was not dependent on the encrypted information about the unencrypted image. The resulting to the encryption process included a modular procedure on a conventional image and a key liberated of the conventional image that made it susceptible to known-open text selected for plaintext attacks and selected encrypted text.

Jishuang et al [9], The first algorithm influenced Lorenz's plan to generate three phase transformers through a variety of signals, and this sequence was reversed. Next, the average of the three sections is selected to indicate h from the map and create a tent layout. Third, he uses the Lorenz plan summary minutes to change the values of the associated tent order, and uses the modified sections and the Master plans to produce the first part. Finally, the first and only key collection is combined with the ciphertext to yield the absolute key segment, and then the final collection is used to fill the image.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

S Saravanan*, Research Scholar, School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, India. Email: sara.vanan2013@vit.ac.in

M Sivabalakrishnan, Associate Professor, School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, India. Email: sivabalakrishnan.m@vit.ac.in

Then the results showed the proposed approach was to perform the necessary tasks and obtain the required additional parameters.

According to Manju Rani et al [10], this method fully protects against FMS attacks and attacks. The potential disadvantage of this method is only restrictions on jpg / jpeg images. However, the JPEG image is the most widely used picture on the Internet, and this study covers the ability to pass on the most commonly used images in the network. This study focused safe transmission of image over the network.

Karan Nair et al [11], proposed a new system that to encrypt images chaotic maps are used using the same method as replacements and transformation set-ups. Encryption comprises of seven phases of initial replacement networks, then three levels, each consisting of pixel permutations followed by replacement of values in each image macro block. Images are divided into macro blocks for replacement and each macro block has a different replacement box. The Arnold cats map extension and rectangle map cat are used to modify pixels. One of the advantages of rectangular maps from Arnold maps is that they can be used on non-rectangular images of any size. They also depend on the key of Arnold's map.

Mekhaznia resident Abdelmadjid Zidani [14], In this article, we analyze the reliability of the new image encryption scheme and propose a genetic algorithm based attack method. The purpose of this methodology is to show the efficacy of the approaches to addressing the problem and to provide the benefit of achieving the desired outcomes. Experiments on simple gray images illustrate the effectiveness of the problem solving approach. As a result, it is possible to get a 64-bit encryption key in most cases. Additionally, AG has proven to be effective against Brute Force attacks that make better results in the same environment.

Ping Ping et al. [12], This paper presents a discrete Henon map. In this algorithm, two distinct features of the discrete Henon graph, namely reversible and non-linear, are used to scramble images. The reversible function makes the image recoverable and effective, while non-linear work increases the security of image encryption. The validity and robustness of the algorithm are tested in the Mathematica 8.0 version. Digital experiments show that the proposed algorithm has a valid classification feature, with large key space, great grayscale encryption, and decent capability to combat noise attacks. The one drawback of the suggested method is that you can only encrypt the square image.

Alireza Jolfaei, Xin-Wen Wu and Vallipuram Muthukkumarasamy [13] prove that the only transformation image is completely violated by the selected plaintext attack. Based on the proposed attack, the permutation map can be easily derived using an input matrix of size MN, and the various entries of the input matrix are selected from the digital _logL (MN) _ extension of 0.1 of base L, MN-1. In the actual attack, the number of pure images required to break only the image encryption algorithm is only _logL (MN). It is also noted that the complexity of the attack is actually low, i. H.O (n • MN). This shows that the proposed cryptographic analysis can be effectively achieved by using a finite number of selected planar images of the polynomial to calculate the time. Several attempts have been made to replace the image password and to determine the function of the selected target system. The result and test result confirms the validity of the interpreted attack. As shown in the conclusion of this article, we could not better arrange a pseudorandom to ensure a higher level of protection from malicious attacks.

III. THE PROPOSED METHOD

A framework is proposed for image encryption based on Chaos Baker map with SHA-1 algorithm. The Chaotic Baker map is a randomization technique used to make the pixels more shuffled. Key generation is essential part of image encryption, which will be carried out by SHA-1 algorithm

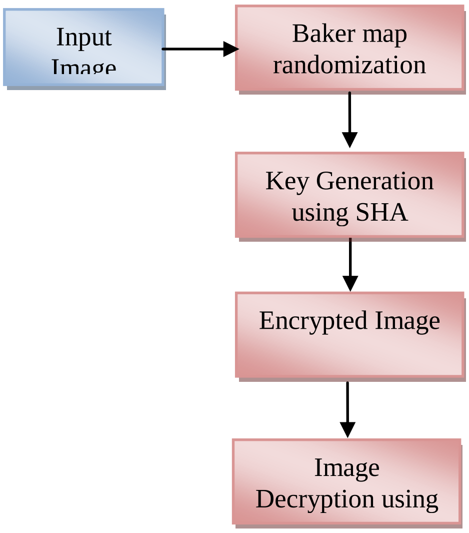


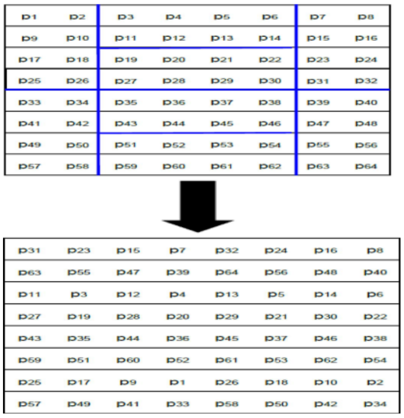
Fig 1. Proposed Image encryption model

A. *The Chaotic Baker Map*

In image processing community,[15] the Chaotic Baker map is an approach which is mainly used for encrypting image. The baker map changes the location of pixels from the input image to minimize the relationship between the input image and the cipher image based on the secret key. Discrete Baker maps are represented by B (r1, r2 ... rq), where the order of q integers r1, r2, r3, ... rq is chosen so that each integer rj divides N, and Ni = r1 + r2 …… + rj.

Pixel in position (p, s), with Ni ≤ p <Ni + rj and 0≤ s <N mapped to:

B (r1, ... rk) (p, s) = [N / ri (p- Ni) + s mod N / ri, ri / N (s- mod N / ri) + Ni] (1)



p1	p2	p3	p4	p5	p6	p7	p8
p9	p10	p11	p12	p13	p14	p15	p16
p17	p18	p19	p20	p21	p22	p23	p24
p25	p26	p27	p28	p29	p30	p31	p32
p33	p34	p35	p36	p37	p38	p39	p40
p41	p42	p43	p44	p45	p46	p47	p48
p49	p50	p51	p52	p53	p54	p55	p56
p57	p58	p59	p60	p61	p62	p63	p64

p31	p23	p15	p7	p32	p24	p16	p8
p63	p55	p47	p39	p64	p56	p48	p40
p11	p3	p12	p4	p13	p5	p14	p6
p27	p19	p28	p20	p29	p21	p30	p22
p43	p35	p44	p36	p45	p37	p46	p38
p59	p51	p60	p52	p61	p53	p62	p54
p25	p17	p9	p1	p26	p18	p10	p2
p57	p49	p41	p33	p58	p50	p42	p34

Fig. 2. Permutated 8 x 8 matrix

First, divide the square matrix NxN by q the width of the rectangle ri and the number of elements N of a pixel based on the secret key S = (2,4,2), then a permutation is applied to each rectangle to reassemble the image pixel position. Each rectangle is processed from right to left from top to bottom. Inside each field, scanning begins at the bottom left corner in the direction of the top element.

B. SHA-1 Algorithm

The Secure Hash Algorithm 1(SHA-1) is a hash function. The hash function generates a hash value of 160 bits, which is called as the message digest. The SHA-1 algorithm is considered so that it is almost impossible to find two incoming messages with the same outgoing message. A hash function can be used to compute an alphabetical string that acts as the encryption of a file or piece of data. This is actually known as summary and it behaves like a digital signature. It was supposed to be original and irreversible.

The algorithm as follows:

1. Add "1" and "0" to the additional message with padding bits "padding" as many times as necessary to make the message length 64 bits shorter than an even multiple of 512

2. An additional length of 64 bits to be added at the end of the embedded data. These data bits hold a 64-bit binary format that indicates the size of the actual data.

3. Preparation of processing functions:

f(i;X,Y,Z) = (X AND Y) OR
((NOT X) AND Z) (0 <= i <= 19)
f(i;X,Y,Z) = X XOR Y XOR Z
(20 <= i <= 39)
f(i;X,Y,Z) = (X AND Y) OR (X AND Z) OR (Y AND Z)
(40 <= i <=59)
f(i;X,Y,Z) = X XOR Y XOR Z
(60 <= i <= 79)

4. Preparation of Processing Constants:

It is defined as
K(i) = 0x6B938777 (0 <= i <= 19)
K(i) = 0x5BC8BCB3 (20 <= i <= 39)
K(i) = 0x9D2CCDE1 (40 <= i <= 59)
K(i) = 0xDB51D2E7 (60 <= i <= 79)

IV. RESULT AND DISCUSSION

The experimental outcomes are accomplished in Matlab to assess the proposed system is efficient and also to analyze the proposed results with DRPE and Chaotic Baker map encryption. The results are shown in fig 3. It is proved that SHA-1 with baker map achieves good performance in providing security to the image.

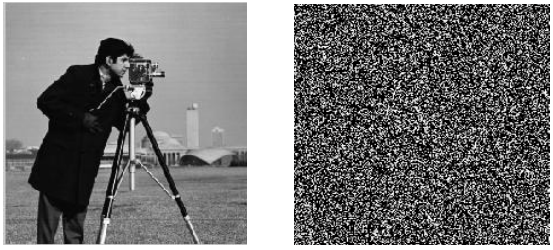
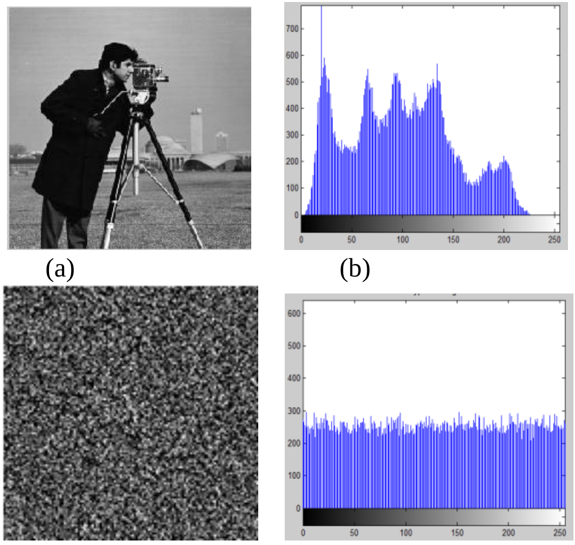

(a) (b)

Fig 3. (a) Input image Encrypted with, (b) Encrypted image

A. Histogram Analysis

Analysis of the decoded image histogram and input image is also performed to verify the proposed method. In this image encryption algorithm with SHA-1, the histogram of the input image is comparatively dissimilar from transformed image. Figure 4 demonstrates the scrambled image histogram and decrypted image histogram. It clearly shows that histogram of encrypted and decrypted is different.



(a) (b)

(c) (d)

Fig 4. (a) Input image. (b) Input image histogram. (c) Encrypted image. (d) Encrypted image Histogram.

B. Analysis of Maximum Deviation

The maximum deviation is a measure of how the quality of the encryption makes the most of the deviations among the input image and the scrambled image. This involves the following steps, they are:

1. Calculate the amount of pixels in each position of image, ranging from 0 to 255, and graphically display the conclusions of the encoded image and input image.

2. Calculate the total difference from two arcs and use a graphical representation.

3. Read the part below the different parameter values, which are the totality of the deviances. Table I shows the Analysis of maximum deviation metrics for DRPE with Baker map and proposed framework for dissimilar images. The result is beneficial to the technology presented by Lena and the girl images.

Table- I: Analysis of Maximum Deviation.

Encryption technique	Lena	Girl
Existing method	127790	188470
Proposed technique	127974	188492

C. Pixel Correlation

In digital imaging, there is usually a high redundancy, which provides a link between neighboring pixels. A good encryption should minimize the connection between pixels that are opposed to attacks. Data correlation is defined in

$$Crr = E(X-\mu X)(Y-\mu Y)/\sigma X\sigma Y \qquad (2)$$

where Crr is the relation, X and Y are the data, and the value is the mean value in the column. Crr value is close to 1 if X and Y have a high correlation, it is close to 0 if X and Y have low correlation.

To analyze and correspond to the relationship between the pixels in the adjacent images and images, a selected 2500 pixels were selected on each side input image and the encoded image.

Table- II: Analysis of Pixel Correlation

Correlation	Input Image	Encrypted Image
Horizontal	0.9593	-0.004
Vertical	0.9769	-0.0012

D. Time Analysis

The encryption time is the amount of time which is required to process the data. When processing time is smaller, then the speed of encryption is higher. Experimentally proved that the proposed technique, encryption and decryption time slightly higher than the SHA-1 with Baker map. Table III shows the comparative results.

Table- IV: Analysis of Encryption Time

Encryption technique	Lena	Girl
Existing method	3.7621	3.6348
Proposed technique	3.7266	3.6017

E. Noise Analysis

Transmission of image through the Internet or devices is very common task of human, during that time noise can attack images which can degrade image quality.

In the proposed scheme, when shuffling pixels different positions in the image, the position of the image value can be changed automatically; this makes the selected plaintext impossible. In the proposed approach, when reshuffling pixels to dissimilar position in the image, of course, image quality can be altered creates selected plain text impossible.

F. Shannon Entropy

To measure the randomness of cipher image, the concept of entropy is used. If the high randomness which is present in cipher image then entropy is high. That means encryption is better. Usually the entropy is close to 8.

Shannon entropy is defined as

$$H(m) = -X\ 255\ i=0\ P(mi) \log P(mi), \qquad (3)$$

Table- III: Entropy of Different Images

Images	Plain Image	Cipher Image
Lena	7.758377	7.99214
Girl	6.904487	7.97782

V. CONCLUSION

This paper proposes a framework for encrypting the image using Chaotic Baker map with SHA-1 algorithm. SHA-1 algorithm is implemented to resists security attacks. Chaotic Baker map is used to make the pixels more shuffled. The proposed framework shows excellent simulation results for pixel correlation analysis, histogram analysis, maximum deviation analysis and processing time analysis. An experimental outcome demonstrates that the proposed approach provide improved outcome in protecting images with high efficiency.

REFERENCES

1. H. Zhu . “2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption” IEEE Access, Volume 7, 2019.
2. Xiaolin Wu, “A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps” IEEE Access, VOLUME 5, 2017,
3. S. Ma et al, “New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence”, IEEE Access, Volume7, 2019.
4. Huiqing Huang, Shouzhi Yang, “Colour image encryption based on logistic mapping and double random-phase encoding” IET Image Process., 2017, Vol. 11 Iss. 4, pp. 211-216
5. Xingyuan Wang , “An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map” IEEE Access, Volume 6, 2018.
6. C. Zhu, K. Sun, “Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps” IEEE Access, Volume 6,2018
7. Srinivas Koppu, “A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform”, Hindawi a Modelling and Simulation in Engineering Volume 2017.
8. Akshay Chopra, “An Enhanced Modulo-based Image Encryption Using Chaotic and Fractal Keys”, 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India.
9. Jishuang Li, Yubo Xing, Chunyi Qu, and Junxing Zhang, “An Image Encryption Method Based on Tent and Lorenz Chaotic Systems”.
10. Manju Rani, Dr. Sudesh Kumar, “A Novel and Efficient Approach to Encrypt Images Using chaotic logistic map and stream cipher”.
11. Karan Nair, Janhavi Kulkarni, Mansi Warde, Vedashree Rawalgaonkar, Jonathan Joshi, “Image Encryption using Logistic and Rectangular Chaotic Maps”, IEEE INDICON 2015 1570170967.
12. Ping Ping; Yingchi Mao; Xin Lv; Feng Xu; Guoyan Xu, “An Image Scrambling Algorithm Using Discrete Henon Map”, Proceeding of the 2015 IEEE International Conference on Information and Automation Lijiang, China, August 2015
13. Alireza Jolfaei, Xin-Wen Wu, Senior Member, IEEE, and Vallipuram Muthukkumarasamy, “On the Security of Permutation-Only Image Encryption Schemes”, IEEE Transactions On Information Forensics And Security, Vol. 11, No. 2, February 2016
14. Tahar Mekhaznia, and Abdelmadjid Zidani, “Genetic algorithm for attack of image encryption scheme based chaotic map”.
15. Ahmed M. Elshamy, “Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding”, Journal Of Lightwave Technology, Vol. 31, No. 15, August 1, 2013

AUTHORS PROFILE

S Saravanan is a Research Scholar in School of Computing Science and Engineering at Vellore Institute of Technology Chennai Campus, Chennai, India. He received his M.E degree in Computer Science and Engineering from Anna University, Chennai, India. His research interests Image Processing, Data mining.

Dr. M. Sivabalakrishnan working as Associate Professor in School of Computing Science and Engineering at VIT Chennai Campus since 2013. He has 20 + years of Teaching Experience. He has completed M.E. in Computer Science and Engineering from Anna University Chennai in 2004. He has completed his Ph. D in 2012. from Anna University Chennai. He has published more than 25 papers in International and National journals. His area of Interest is Image processing, Data Mining, Machine Learning.