Image Encryption Algorithm based on Particle Swarm Optimization and Chaos Logistic Map

Hussain Alibrahim
Department of Computer Science
North Dakota State University
Fargo, USA
hussain.alibrahim@ndsu.edu

Simone A. Ludwig
Department of Computer Science
North Dakota State University
Fargo, USA
simone.ludwig@ndsu.edu

***Abstract*—With the fast growth of data transmission and sharing technology, image encryption is becoming a widely discussed topic in the field of information security. In this paper, Particle Swarm Optimization (PSO) algorithm used with Chaos Logistic Map to create encryption algorithm. The purposed algorithm benefitted from PSO advantage such as search large space fast, short computation time, higher probability finding the global optimization value and PSO do not overlap solutions or mutate to find best encryption image. Furthermore logistic map equation used for confusion and diffusion operations. The algorithm start by creating several encrypted images – these are the particles for PSO - and logistics maps, the encryption key used is based on the plain image only. The optimization step is measuring the pixels correlation, where lower correlations value is the best value, and this serve as fitness function. The simulation results of the proposed algorithm indicate an effective encryption process. In addition, the security analysis illustrates the ability of this algorithm to provide a satisfying level of security in comparison with other image encryption schemes.**

***Index Terms*—Image Encryption, Particle Swarm Optimization, PSO, Chaos Logistic Map**

I. Introduction

In now days internet is used for making different communication type over the world, this interactions has different shape based on its goal. It could be family call, educational session, work meeting or even military secret conference. In special condition of people live, like covid 19 pandemic, it become mandatory for people to meet using the internet and this including top people in countries like presidents. Unfortunately, this media is not safe and there are a lot of expert hacker or attacker trying to access other data for different purposes. Images is one type of this data that used to be shared, these images my involve in personal privacy information, sensitive trading data, military secrets or even national security secret. Protecting image information over the network or internet focused in 3 main goals of security [1]:

- **Confidentiality:** Image data is not accessible from unauthorized user.
- **Integrity:** protect image data from unauthorized modification.
- **Availability:** Image is available when its needed by authorized user.

Compared to the text data, digital image's characteristics as large amount of data, strong correlation, big data redundancy, storge format and others make the traditional encryption methods, such as Data Encryption Standard (DES), International Data Encryption (IDEA) and Advanced Encryption Standard (AES) are not so suitable for image encryption. These algorithms can not resist statistical, differential and other attacks and easily fail. Every image encryption system is mainly composed of two parts: 1) secret key, and 2) encryption algorithm. According to the basic principle of cryptology, a cryptosystem should be sensitive to the secret key. One way to accomplish this requirement is usage of ideally and truly random key generation mechanism. In other words, based on secret keys, pseudo-random sequences are produced for encryption of the image. The pseudo-random key stream is then used to mask and encrypt each plain-image pixel sequentially in the encryption algorithm.

Therefore, A variety of image encryption schemes have been proposed to achieve the goal of secure image such as [1]: Block based using substitution [2] or permutation [3], Bit Transform using Arnold [4] or Angular [5], Conventional based such as AES [6], DES [7] or RC5 [8], Chaos based algorithm such as Map [9] one dimensional Chaos [10] or Hyper Chaos [11] Including tho these, there are miscellaneous based like DNA sequence [12], genetic algorithm [13], Double phase Random Encoding [14]. These are some exist algorithm used in image encryption and there are a lot exist not listed du to the nature of this paper.

This paper organized as follow, related work section, then detailed the approach used in this paper ,then define the quality metrics used to evaluate this work, then describe the test and results and finally conclude the paper .

II. Related Work

In [2] a novel variant of Substitution-Box used to encrypt the images. The main contribution was a novel and simple modular approach to construct nonlinear S-boxes and dynamic permutation operation is applied to the values of S-box to create more confusion. For S-box having size $n \times n$, the novel transformation function represented in math as: $L(z) = [A \times z + B]MOD(2^n + 1)$ $z \varepsilon N$ where $N = \{0, 1, 2...255\}, O = \{1, 3, 5, ...255\}$, $A \varepsilon O$ and $B \varepsilon N$.

Each S-box method need to find the Multiplicative Inverses (MI) for each value in box, in this paper simpler approach

used to find MI instead of using Galois field which consider complicated process. this approach represented mathematically as $MI(L(z)) = L(z)MOD(2^n + 1)$. MI used in permutation process to make it dynamic with large search space, i.e for S-box of size 8×8 the total number of permmtation is $2^{16}!$. this make it very convusion process. Then experiment conducted to evaluate different statistical performance measures such as histogram analysis, difference analysis, similarity analysis..etc. using benchmark images. The results compared with others work and found out this algorithm can improve image encryption using S-box.

In [10], hyper algorithm based on Genetic algorithm and DNA sequence used in image encryption. DNA sequence elected as it offers greater storage and higher computing capabilities. The encryption method consists of two phases: Transposition or Scrambling phase and Substitution phase. In the first phase, pixel locations are altered using GA to reduce the correlation among adjacent pixels. In substitution phase, the pixels are replaced by using XOR operation between the pixel values converted into binary strings and DNA substrings derived from a random DNA string. DNA substrings are used as keys for image encryption. The experimental outcome confirms that the algorithm is simple, fast enough and feasible. Performance analysis declares the robustness of the algorithm against all kinds of attacks and thereby maintaining higher security.

In [15] modern framework presented using the defining of the neighborhood nonlinear map within the Coupled Map Lattices (CML). The outline was connected to the instrument of permutation-diffusion. The encryption scheme chaos considered that the merits of spatiotemporal chaos and the Nonlinear Chaotic Algorithm (NCA) is a great execution and has profoundly eccentric chaotic sequences.

In [16] an effective scheme for image encryption presented dependent on the settled nested chaotic map and Deoxyribonucleic Acid (DNA) utilizing (e Secure Hash Algorithm (SHA-256) to produce the initial states of the chaotic attractor, and introduced a new chaotic system dependent on Julia's fractal procedure, tumultuous attractors, and logistic map in a complex set.

In [30] New form of PSO has been developed using chaotic maps (tent map and logistic map) and Gaussian mutation. The initial form of PSO is easily stacked into the local optima and appears early convergence during the search process. To address these problems chaotic map is employed to initialize uniform distributed particles so as to improve the quality of the initial population, which is a simple yet very efficient method to improve the quality of initial population. Furthermore, Gaussian mutation mechanism based on the maximal focus distance is implemented to help the algorithm escape from the local optima and make the particles proceed with searching in other regions of the solution space until the global optimal or the closer to optimal solutions can be found. Experimental results on two benchmark functions demonstrate the effectiveness and efficiency of the PSO algorithm proposed.

In [31], PSO and five popular chaotic maps: logistic, singer, sinusoidal, tent, and Zaslavskii has been integrated to build effective docking applications. These programs are routinely used in structure-based drug design to find the optimal binding pose of a ligand in the protein's active site. These programs are also used to identify potential drug candidates by ranking large sets of compounds. Pose prediction experiments indicate that chaos-embedded algorithms outperform docking algorithms in ligand pose root mean square deviation RMSD, success rate, and run time. In virtual screening experiments, the purposed system achieved a very significant five- to sixfold speedup with comparable screening performances to AutoDock Vina in terms of area under the receiver operating characteristic curve and enrichment factor.

III. Our Approach

This paper approach used Chaotic Logistic Map with PSO to implement the encryption algorithm used. Chaos theory [17] in math is "the study of apparently random or unpredictable behavior in systems governed by deterministic laws A more accurate term, deterministic chaos, suggests a paradox because it connects two notions that are familiar and commonly regarded as incompatible" these notationes are randomness and deterministic behavior. Chaos is a dynamical systems whos the apparent randomness of chaotic complex systems, there are underlying patterns, interconnectedness, constant feedback loops, repetition, self-similarity, fractals, and self-organization. The most common element in chaos systems is a very high degree of sensitivity to initial conditions and to the way in which they are set in motion.

In general, chaos-based image encryption algorithms consist of two steps: pixel permutation and pixel diffusion. The pixel permutation changes pixel position, while the pixel diffusion alters pixel values where a change in a pixel will spread almost to other pixels of entire image. Contributed by the sensitivity properties of chaotic system, chaos-based image encryption algorithms generally achieve good security performance.

Logistic map [18] is one polynomial mapping of degree 2 popularized and published by biologist Robert May in 1976 as a discrete-time demographic model , this map can be expressed as Equation 1:

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

where X_n is the ratio of existing population to the maximum possible population, it can be any value between 0 and 1, r is the values of interest and its between 0 and 4.

Logistic map behavior [19] regard less of initial population X value can be determined depending on r value. Behavior can be summarized as follow:

- r value less than 1.0 the population will end to zero.
- r value between 1.0 and 2.0 the population will stabilize on fixed value after few iteration.
- r value between 2.0 and 3.0 the population will stabilize on fixed value after fluctuates in first few iteration.
- r value between 3.0 and 3.45 the population will fluctuates between 2 value

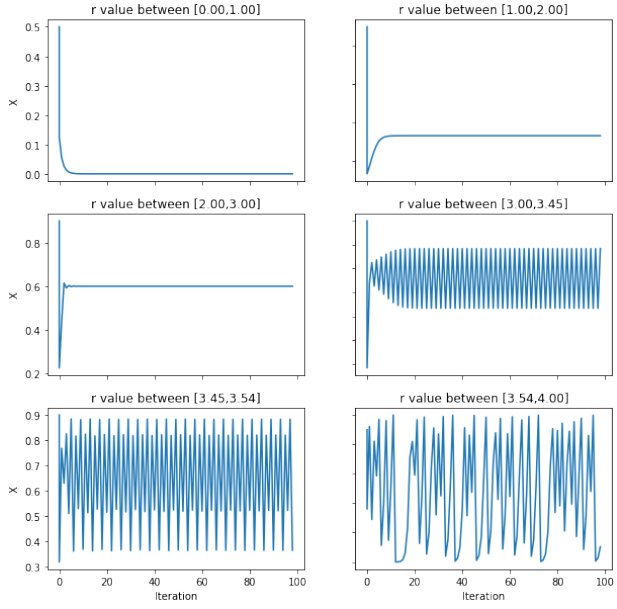


Fig. 1: Logistic Map Behavior

- r value between 3.45 and 3.54 the population will fluctuates between 4 value
- r value between 3.54 and 4.0 population will exhibit chaotic behavior.

Figure 1 show the behavior for logistic map in 100 iteration using different value of r regardless of initial population value.

The main work frame in this paper is PSO. PSO [20] is a computational method that used in problem optimization. It iteratively trying to improve a candidate solution by improve fitness function value. it works based on population of candidate solutions that called particles, these particles keep moving in search space and update velocity and position values – that both randomly initialize before iterative begin – by using stander equations. Equation 2 is for velocity update:

$$v_i(t+1) = w \times v_i(t) + c_1 \times u_1 \times (Pbest_i(t) - X_i(t)) + c_2 \times u_2 \times (Gbest_i(t) - X_i(t)) \quad (2)$$

and Equation 3 for position update:

$$X_i(t+1) = X_i(t) + v_i(t+1) \quad (3)$$

All particles move with guide of global best position that shared between swarm members after each iteration. Global best also updated by compare the value with all particles position value and take best particle position in each iteration if its better than old global best.

Our approach initialization phase, as in algorthim 1 starts by reading the image, then based on population size same number of encrypted images will be generated, these encrypted images are the particles in PSO. Each particle position and velocity are dependent on random, this number value is less than image pixels number. In addition to particle position and velocity, image coefficient correlation is measured that value used to define particle best position. Correlation coefficient defination and how its clculated desriped in Simulation Experiment section. After creating all particles and set particle best positions the swarm global best is updated too.

Algorithm 1: Initialization

Input : Plain Image
Output: Encrypted Image

Read image (I) of size ($M \times N$)
Read population size (P)
for p *in* P **do**
  X = random number $\leq (M \times N)$
  key = GenerateKey(X, I)
  $eimage$ = Encrypt($image, key$)
  $velocity(p) = \lfloor X/M \rfloor$
  $position(p) = X$
  $p\_best\_pos = X$
  p_b_ccf = CorrCof(p)
  if $g\_best > p\_b\_ccf$ **then**
    $g\_best = p\_b\_ccf$
    $g\_best\_pos = p\_best\_pos$
  end
end

The initialization phase use two methods which are generate key and the encryption methods. The Generate keys - as in Algorithm 2- objective is to return encryption key of size 40 bits that used in encryption process based on the plain image and random value only. using the random number from input parameter, the method will figure out the rows and column of the first pixel, then it will read diagonally four additional pixels, convert each pixel value to binary value, concatenate all binary values and finally return it as encryption key. For each particle this random number has to be saved since it's the only key required for decryption process too.

Algorithm 2: Generate Key

Input : Number X
Image I (Size ($M \times N$)
Output: Key

$r = \lfloor \frac{X}{M} \rfloor$
$c = N \mod X$
$key =$ $concatenate(binary(I(r,c)), binary(I(r+1, c+1))$ to $binary(I(r+4, c+4)))$
return key

The encryption process as in Algorithm 3 used logistic map equation. As described earlier for this equation initial population X_n and increasing rate r values are predefined.

the encryption key used to calculate X_0 value as Equation 4.

$$X_0 = \frac{key[1] \times 2^{39} + key[2] \times 2^{38} + ... + key[40] \times 2^0}{2^{40}} \quad (4)$$

The r value used is from category where logistic map behave chaotic. After that loop over each pixel of image and XOR it with $(X_0 \times 256)$, and the result is an encrypted image returned to initialization phase as particle.

Algorithm 3: Encryption Process

input : Key key
Image img $(M \times N)$
Output: Encrypted Image eimge

X_0 (calculated as equation 4 using key)
for $i = 1$ *to* M **do**
  for $j = 1$ *to* N **do**
    $eimg(i, j) = \lfloor (X_0 \times 256) \oplus img(i, J) \rfloor$
  end
end
return eimg

Last step in this approach is to optimize the solution using PSO, that mean finding the lowest value of coefficient correlation of image,for this in each iteration update particle velocity, position using equations 2, 3 and calculate the coefficient correlation value. Calculation process for coefficient correlation use index value of the particle as random number, particles as image, then generate the keys, encrypt images, and finally calculate correlation coefficient value. After that update, the particle best position and swarm global best position. This process continued in each iteration. At last return image with best global position as encrypted images.
The decryption process is revised of encryption process, it needs the random number selected at encryption process and the chaotic function logistic map with same r values.

IV. Simulation Experiment

To test this approach, algorithm implemented in python and different analyses measured to show the strength of this algorithm. its tested using eight benchmark images, that are: Lena, Peppers, Baboon, Barbara, Gold Hill, Cameraman, Fruits and Sail Boat. All the tests applied in grayscale images of size 512×512 version. This algorithm can be applied to color image and use RGP color analysis instead of one color.

A. Correlation Coefficient

As in [26], Pearson correlation coefficient (CCF) is a statistical matric the measure the strength and direction of a linear relationship between any two random variables. It has been used in many different filled such classification, clustering, finance analysis, and biological research. In this paper approach used as fitness function of PSO, that aim to receive image with very low correlation coefficient value - close to 0- . in plain image an unencrypted one, any adjoining pixels have very high correlation, that mean destroyed this correlation lead to save image information and data from any statical attack that can be used. CCF is the covariance of two variables, divided by the product of their standard deviations; thus it is essentially a normalized measurement of the covariance, such that the result always has a value between -1 and 1. The CCF values close to 1 and -1 mean high correlation, while value close to 0 means no correlation at all. Mathematically CCF calculated as Equation 5

$$ccf = \frac{N \sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{(N \sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2) \times (N \sum_{i=1}^{N} y_i^2 - (\sum_{i=1}^{N} y_i)^2)}} \quad (5)$$

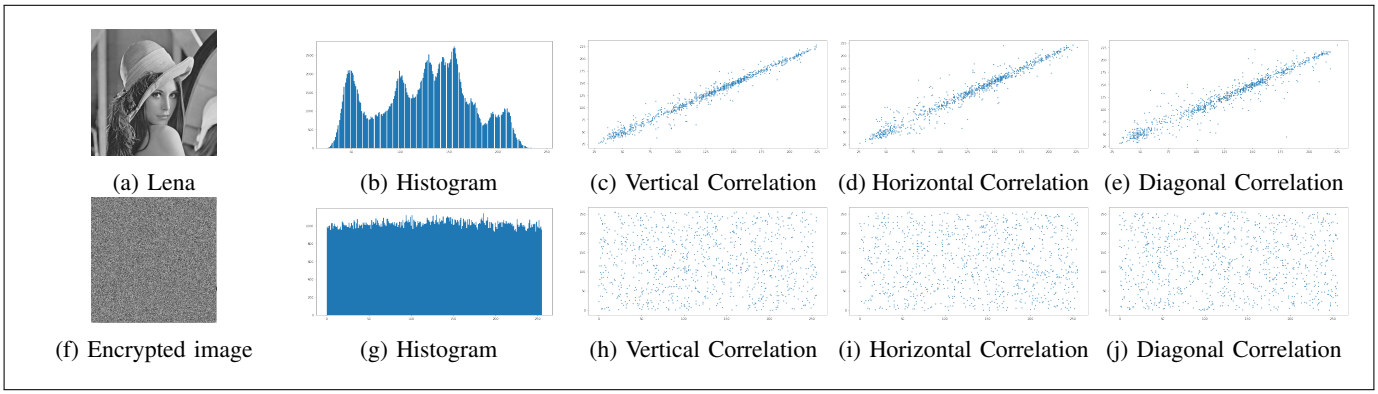
wher N is the total number of pixcels, x and y are any adjacent pixcel value.
Table I show the correlation value and compare it with results from different papers using different technique. In most of the cases this paper approach show higher performance in destroying the correlation, for example in Lena image the value was around $9.5 * 10^{-8}$ where in [25] was 6.8×10^{-6} and this was the nearest value. Peppers image is another example with ccf value 6.1×10^{-6} while in [21] was only 5.2×10^{-5}. In Gold Hill image, [25] has better value than our value by small difference.

TABLE I: Pearson Correlation Coefficient

image	Our	Ref. [21]	Ref. [25]	Ref. [2]
Lena	9.46E-08	4.83E-05	6.82E-06	NA
Peppers	6.11E-06	5.25E-05	2.46E-04	3.00E-04
Baboon	2.96E-06	5.15E-04	NA	NA
Barbara	1.65E-05	2.18E-04	2.26E-04	1.30E-03
Gold Hill	3.00E-05	NA	2.93E-05	2.00E-04
cameraman	2.48E-05	NA	NA	NA
Fruits	1.69E-05	NA	NA	NA
Sail Boat	1.03E-05	5.15E-05	1.44E-06	NA

While Table I shows the pixel correlation with all adjacent pixel, Table II shows more specific information. Its display the result of pixels correlation with vertical adjacent pixels alone, horizontal adjacent pixels and diagonal adjacent pixels separately. For example Lena image after encryption process has 0.001 vertical correlation, 0.0002 horizontal correlation and 0.0006 diagonal correlation, while [22] values are: -0.04, 0.0005 and 0.003. Anther example is Fruits images with values 0.008,0.004 and 0.002 while [24] values are -0.0155, -0.0129 and 0.0012. In most result this algorithm perform better than other except horizontal correlation for camera man image. Figures 2 - 5 visualize vertical, horizontal and diagonal correlation coefficient for Lena, Barbara, Camera man and Sail Boat in image c, d and e before the encryption process, and clear relation can be see in all images. Images h, i, j shows the correlation after the encryption process, from these image its clear that correlation values are at minimal value.

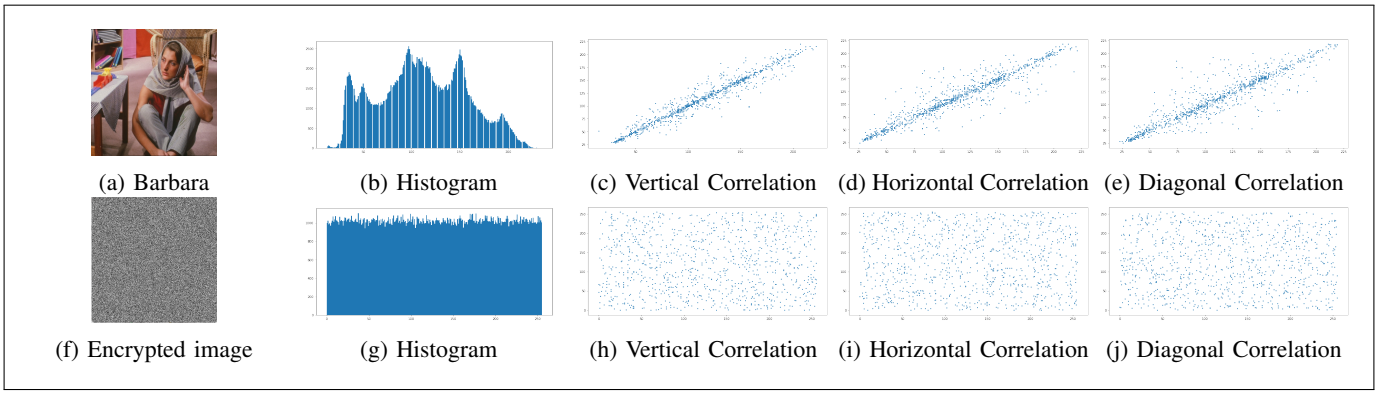
With these results of correlation coefficient, the PSO with logistic map equation prove that they can improve the security in image encryption and destroyed almost all the relation between image pixels.



(a) Lena (b) Histogram (c) Vertical Correlation (d) Horizontal Correlation (e) Diagonal Correlation

(f) Encrypted image (g) Histogram (h) Vertical Correlation (i) Horizontal Correlation (j) Diagonal Correlation

Fig. 2: Lena Images and Encrypted Image with Histogram and Coefficient Correlation



(a) Barbara (b) Histogram (c) Vertical Correlation (d) Horizontal Correlation (e) Diagonal Correlation

(f) Encrypted image (g) Histogram (h) Vertical Correlation (i) Horizontal Correlation (j) Diagonal Correlation

Fig. 3: Barbara Images and Encrypted Image with Histogram and Coefficient Correlation

TABLE II: Vertical, Horizontal & Diagonal Correlation

	Correlation			Reference [22]		
Image	V-Corr	H-Coor	D-Corr	V-Corr	H-Coor	D-Corr
Lena	0.001142	0.000224	0.000570	-0.03911	0.00047	0.00305
Peppers	0.002927	0.001750	0.002813	0.04321	0.00198	0.02547
Baboon	0.002717	0.002981	0.000898	0.00285	0.00318	-0.00294
Barbara	0.001748	0.001806	0.000497	NA	NA	NA
Gold Hill	0.008919	0.000788	0.004296	NA	NA	NA
Cameraman	0.001219	0.006339	0.000803	0.0019	0.00212	-0.00205
Fruits	0.007627	0.004159	0.002185	NA	NA	NA
Sail Boat	0.000966	0.009781	0.007364	NA	NA	NA

B. Histogram Analysis

An image histogram [27] is a graphical representation of the color distribution for an image. Color theories describe each color by using three primary way:

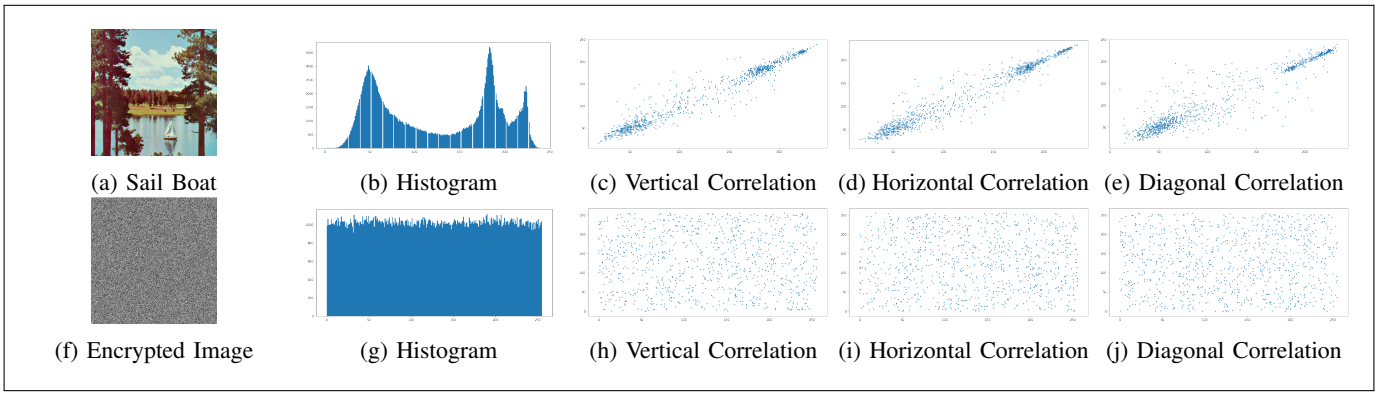
- **Hue:** which means the color only.
- **Saturation:** is the intensity or purity of a hue.
- **Lightness:** is the relative degree of black or white mixed with a given hue.

In this paper grayscale image used, so gray histogram analysis tested which is the statistical numbers of each different gray level from 0 to 255 of all picture pixels. This test measure the level of gray color in image before and after encryption and will plot the histogram for each. This distribution of pixels is an indicator of image content. A perfect encrypted image has random-noise image tends to ideally flat or uniform distribution of pixels. Figures 2 - 5 subfigure a shows the original image, b shows the original image histogram, f shows the image after encryptions and g shows the histogram of encrypted images.

Its clear that each plain image which is meaning full one has a histogram that has several peaks and normal distribution of gray level. However, the corresponding encrypted images are quite noise and meaningless for a casual observer, thus illustrating the indistinguishability of an encrypted image. Moreover, an effective encryption effect can also be confirmed by analyzing their histogram plots shown in subfigure b. The histograms of encrypted images depicts that the distribution of pixels in each encrypted images are more flat than their plain images histograms and substantially better than the histograms of encrypted images obtained in [25].

C. Image Entropy

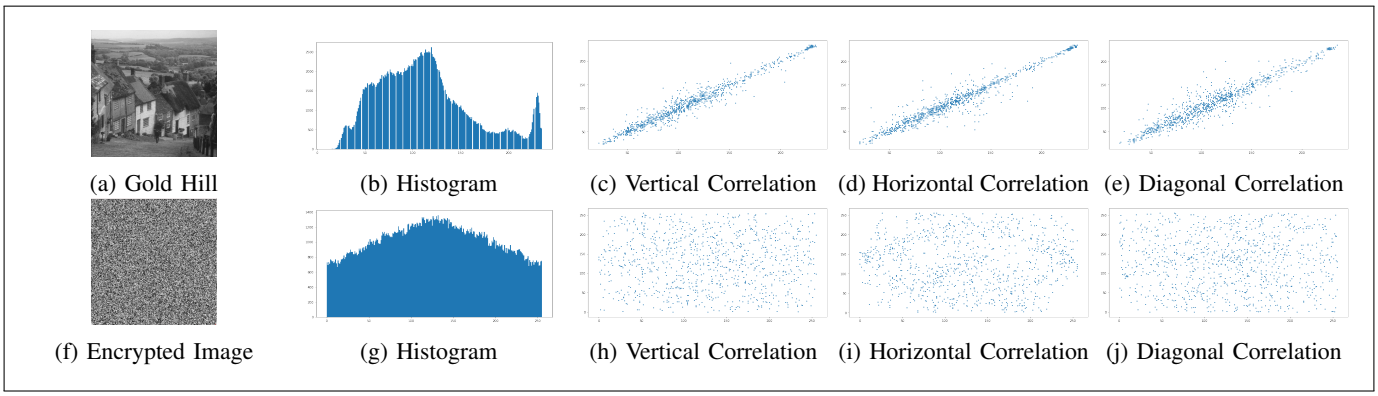
Shannon entropy [28], introduced in 1948 by Claude Shannon, in his paper " A Mathematical Theory of Communication". Since then, Shannon entropy has been widely used in the information sciences. Shannon entropy is a measure of the uncertainty associated with a random variable. Specifically, Shannon entropy quantifies the expected value of the infor-



(a) Sail Boat (b) Histogram (c) Vertical Correlation (d) Horizontal Correlation (e) Diagonal Correlation

(f) Encrypted Image (g) Histogram (h) Vertical Correlation (i) Horizontal Correlation (j) Diagonal Correlation

Fig. 4: Sail Boat Images and Encrypted Image with Histogram and Coefficient Correlation



(a) Gold Hill (b) Histogram (c) Vertical Correlation (d) Horizontal Correlation (e) Diagonal Correlation

(f) Encrypted Image (g) Histogram (h) Vertical Correlation (i) Horizontal Correlation (j) Diagonal Correlation

Fig. 5: Gold Hill Images and Encrypted Image with Histogram and Coefficient Correlation

mation contained in a message. in image encryption process level of gray in image – represented in histogram – is the information of the message need to be encrypted. In original image the entropy value represents the amount of data to be encrypted to make the image highly random, while in encryption image the value represent the amount of data need to decrypted to get meaning full image. the maximum value of entropy is 8 since $log_2 256 = 8$.
entropy for image X can be calulcated using Equation 6:

$$E(X) = \sum_{l=1}^{L-1} \frac{n_l}{T} Log_2 \frac{n_l}{T} \tag{6}$$

where L is gray scale from 0 to 255, T is the number of pixcels and n_l is the l-th pixcel value.

By looking at Table III, this approach return very high entropy values – even compare to original image. For example Lena plain image has entropy value 7.4455, Barbara 7.6278, Peppers 7.5982 and Gold Hill entropy value is 7.4778. most of entropy value of encrypted images has value greater than 7.999 which is very high value since the ideal value is 8. Other reference also has great result too, but our approach has better performance almost for all of them except for Camera man image where [22] value was 7.999 and our approach value is 7.997.
These results indicating that this approach is effective enough in raising the randomness in the encrypted images and has strength to resist the entropy based attacks.

TABLE III: Entropy

Image	Entropy	[21]	Ref. [22]	Ref. [25]	Ref. [2]	Ref. [23]
Lena	7.99982	7.99746	7.99930	7.97200	NA	7.90230
Peppers	7.99943	7.99423	7.99940	7.97970	7.57140	7.90240
Baboon	7.99982	7.99664	7.99930	NA	NA	NA
Barbara	7.99936	7.99775	NA	7.98520	7.63210	NA
Gold Hill	7.97502	NA	NA	7.97910	7.48020	NA
Cameraman	7.99739	NA	7.99910	NA	NA	NA
Fruits	7.99928	NA	NA	NA	NA	NA
Sail Boat	7.99921	7.99472	NA	7.97890	NA	7.90190

D. Differential Analysis

Differential attack is a branch of study in cryptography that compares the way differences in input relate to the differences in encrypted output. Primer objective of this analysis is to study block ciphers to verify if changes in plaintext result in any non-random results in the encrypted ciphertext. The importance of random change in ciphertext -if changed in plain text - indicates strength in the encryption scheme. This high randomness level prevents any unauthorized access to the data

from gain information about what was encrypted or how it was encrypted by monitoring data changes.

As for text encryption, the same analysis applied to image encryption to evaluate the algorithm strength and weakness. Thus, the following analyses were conducting over the algorithm purposed in this paper. Further detail about this in [29].

1) Number of changing Pixel Rate (NPCR):

NPCR is quantify the number of pixels change between two encrypted images for same plain image with single pixel change in before second encryption. This process used to evaluate the effect of change in results encrypted image. Assume C^1 and C^2 are the encryption result for same images while C^2 encryption process started after single pixel change in original image. NPCR calculated by construct a tow dimensional array of image pixel size. Each element value in that array is 0 or 1 only, its based whether the pixel value in C^1 and C^2 are equal or not. This can be represented mathematically as Equation 7:

$$D(i,j) = \begin{cases} 0, & C^1(i,j) = C^2(i,j) \\ 1, & C^1(i,j) \neq C^2(i,j) \end{cases} \tag{7}$$

Then use Equation 8 to calculate the NPCR value where T represents total number of pixeles:

$$NPCR = \sum \frac{D(i,j)}{T} \times 100 \tag{8}$$

Table IV show the result of the NPCR value of eight image and compare other work results. seven image NPCR values where above 99.5% and the last one – Baboon- was 99.22%. This results shows that this algorithm result is highly random and simple alert lead to big change in results with difference in more than 99%. Furthermore, this algorithm shows high performance in compared to other work, in most of the test while in some cases like Lean image the result was 99.54% while [22] results is 99.66%.

TABLE IV: NPCR

Image	NPCR	Ref. [21]	Ref. [22]	Ref. [25]
Lena	99.542	99.645	99.664	99.228
Peppers	99.634	99.614	99.629	99.167
Baboon	99.221	99.583	99.644	NA
Barbara	99.609	99.272	NA	99.253
Gold Hill	99.594	NA	NA	99.237
Cameraman	99.660	NA	99.652	NA
Fruits	99.611	NA	NA	NA
Sail Boat	99.583	99.558	NA	99.191

2) Unified Averaged Changed Intensity (UACI):

UACI is a value that determines the average intensity of differences regarding the plain and cipher images. its calculated by summation the difference in pixels between C^1 and C^2. And then divide by multiplication of total number of pixels (T) and largest supported pixel value (F) which is 255. Equation 9 represent the calculation of UACI mathematically.

$$UACI = \sum \frac{|C^1(i,j) - C^2(i,j)|}{F \times T} \times 100 \tag{9}$$

Table V present the result of UACI value achieved by this approach. Most value achieved is greater than 33.4% which means High sensitivity encryption algorithm. Fruits image is an exceptions where its value was around 32%. Compare these results with other works shows this algorithm is stronger in create uncertainty encrypted images in most cases but also as other tests there are some exceptional cases.

TABLE V: UACI

Image	UAC	Ref. [21]	Ref. [22]	Ref. [25]	Ref. [2]	Ref. [23]
Lena	33.454	33.561	33.612	30.147	NA	33.460
Peppers	33.848	33.587	33.601	30.667	33.840	33.430
Baboon	33.637	33.611	33.643	NA	NA	NA
Barbara	33.748	33.554	NA	30.972	33.200	NA
Gold Hill	33.705	NA	NA	30.485	33.130	NA
Cameraman	33.658	NA	33.643	NA	NA	NA
Fruits	32.231	NA	NA	NA	NA	NA
Sail Boat	33.633	33.483	NA	31.159	NA	33.470

V. Conclusion

This paper presents a new algorithm for image encryption. This algorithm utilize the power of PSO in solving optimization problem, and benefited from logistic map chaotic behavior to increase the security level. The algorithm main idea is to find the lowest pixel correlation. it has been implemented in python and tested using eight benchmark images. The encrypted images evaluated using different test which are: pixel coefficient correlation, histogram analysis, entropy analysis, pixel changing rate and unified averaged changed intensity. The results achieved in this algorithm optimum efficacy of the anticipated approach in comparison to other recent image encryption methods. Moreover, the proposed encryption approach demonstrates better performance and higher resistance against analytical attacks in comparison to other works. Hence, the excellence of our encryption approach in terms of mainly CCF, and pixels distributions, entropy, differential analysis is endorsed by the simulation outcomes and analyses.

References

[1] S.Geetha, P.Punithavathi, A.Magnus Infanteena and S. Siva Sivatha Sindhu, A Literature Review on Image Encryption Techniques, International Journal of Information Security and Privacy (IJISP), vol. 12 issue 3 , July-September 2018, doi:10.4018/IJISP.2018070104.

[2] A. H. Zahid, E. Al-Solami and M. Ahmad, A Novel Modular Approach Based Substitution-Box Design for Image Encryption, in IEEE Access, vol. 8, pp. 150326-150340, 2020, doi: 10.1109/ACCESS.2020.3016401.

[3] J.Chen, Z. Zhu, C. Fu, H. Yu and L. Zhang, An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering, vol: 67, pp: 191-204, 2016, doi: 0.1016/j.optlaseng.2014.11.017.

[4] H. Liu, B. Zhao, and L. Huang, "Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling," Entropy, vol. 21, no. 4, p. 343, Mar. 2019.

[5] X. Kang, A. Ming and R. Tao, "Reality-Preserving Multiple Parameter Discrete Fractional Angular Transform and Its Application to Color Image Encryption," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 6, pp. 1595-1607, June 2019, doi: 10.1109/TCSVT.2018.2851983.

[6] P. Sharma, H. Sabharwal, A New Image Encryption using Modified AES Algorithm and its Comparision with AES, International Journal Of Engineering Research & Technology (IJERT) vol: 09, issue 08,August 2020.

[7] S.Kumar and S. Srivastava, Image Encryption using Simplified Data Encryption Standard (S-DES), International Journal of Computer Applications, vol:104, no:2 October 2014, doi: 10.5120/18178-9070.

[8] R. Shahzadi, S. M. Anwar, F. Qamar, M. Ali and J. J. P. C. Rodrigues, "Chaos Based Enhanced RC5 Algorithm for Security and Integrity of Clinical Images in Remote Health Monitoring," in IEEE Access, vol. 7, pp. 52858-52870, 2019, doi: 10.1109/ACCESS.2019.2909554.

[9] X. Chai, Y. Chen and L. Broyde, A novel chaos-based image encryption algorithm using DNA sequence operations, Optics and Lasers in Engineering, vol: 88, pp 197-213, 2017, doi: 10.1016/j.optlaseng.2016.08.009.

[10] S. K. Pujari, G. Bhattacharjee and S. Bhoi, A Hybridized Model for Image Encryption through Genetic Algorithm and DNA Sequence, Procedia Computer Science, vol: 125, pp 165-171, 2018, doi: 10.1016/j.procs.2017.12.023.

[11] S. Liansheng, D. Cong, Z. Xiao, T. Ailing and A. Anand, Double-image encryption based on interference and logistic map under the framework of double random phase encoding, Optics and Lasers in Engineering, vol: 122, pp 113-122 2019, doi: 10.1016/j.optlaseng.2019.06.005.

[12] L. Xingbin, X. Di and L. Cong, Quantum image encryption algorithm based on bit-plane permutation and sine logistic map, Quantum Information Processing, vol: 19 issue 8 , 2020, doi: 10.1007/s11128-020-02739-w.

[13] A. Mansouri and X. Wang, A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme, Information Sciences, vol: 520, pp: 46-62, 2020, doi: 10.1016/j.ins.2020.02.008.

[14] L. Yujia, J. Zhaoguo, X. Xiping, Z. Fuqi and X. Jiahong, Optical image encryption algorithm based on hyper-chaos and public-key cryptography, Optics and Laser Technology, vol:127, id: 106171, July 2020, doi:10.1016/j.optlastec.2020.106171.

[15] C.Y. Song, Y.L. Qiao, and X.Z. Zhang, An image en- cryption scheme based on new spatiotemporal chaos, Optik- International Journal for Light and Electron Optics, vol. 124, no. 18, pp. 3329–3334, 2013.

[16] N. B. Slimane, N. Aouf, K. Bouallegu and M. Machhout, An efficient nested chaotic image encryption algorithm based on DNA sequence," International Journal of Modern Physics C, vol. 29, no. 7, Article ID 1850058, 2018.

[17] Encyclopedia Britannica. 2021. chaos theory — Definition & Facts. [online] Available at: https://www.britannica.com/science/chaos-theory [Accessed 2 May 2021].

[18] M. Ausloos and M. Dirickx, The Logistic Map and the Route to Chaos From the Beginnings to Modern Applications. Berlin: Springer, 2006.

[19] M. T. Akter, Observation of Different Behaviors of Logistic Map for Different Parameters, International Journal of Applied Mathematics and Theoretical Physics, vol: 4, 2018, doi: 10.11648/j.ijamtp.20180403.14.

[20] D. Wang, D. Tan, and L. Liu, Particle swarm optimization algorithm: an overview., Soft Comput 22, pp: 387–408, 2018. doi: 10.1007/s00500-016-2474-6.

[21] M. Ahmad, M. N. Doja and M. M. Sufyan Beg, Security analysis and enhancements of an image cryptosystem based on hyperchaotic system, Journal of King Saud University - Computer and Information Sciences, vol: 33, issue: 1, pp 77-85, 2021, doi: 10.1016/j.jksuci.2018.02.002.

[22] Y. Ibrahim, K. Fahmi, M. Mohamed and S. Ahmed, A New Image Encryption Scheme Based on Hybrid Chaotic Maps, Hindawi, vol:2020, 2020, doi: 10.1155/2020/9597619.

[23] G. Bin and L. Hai-Bo,Image Encryption Application of Chaotic Sequences Incorporating Quantum Keys, International Journal of Automation and Computing, vol: 17, issue:1, 2020, doi: 10.1007/s11633-019-1173-z.

[24] M. Khan and H.M Waseem, A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS ONE vol: 13, no:11, 2018 doi: 10.1371/journal.pone.0206460.

[25] Y. Bedir, K. Fahmi, M. Ahmed and T. Ali, A novel image encryption/decryption scheme based on integrating multiple chaotic maps, American Institute of Physics, vol:10, issue: 7, 2020, doi: 10.1063/5.0009225.

[26] H. Zhou, Z. Deng, Y. Xia and M. Fu, A new sampling method in particle filter based on Pearson correlation coefficient, Neurocomputing, 2015, doi: 10.1016/j.neucom.2016.07.036.

[27] S. Xia, P. Chen, J. Zhang, X. Li and B. Wang, Utilization of rotation-invariant uniform LBP histogram distribution and statistics of connected regions in automatic image annotation based on multi-label learning, Neurocomputing, vol: 228, pp: 11-18, 2017, doi: 10.1016/j.neucom.2016.09.087.

[28] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, Information Sciences, vol 222, 2013, pp 323-342, Doi: 10.1016/j.ins.2012.07.049.

[29] Y. Wu, J.P. Noonan, S. Again, NPCR and UACI Randomness Tests for Image Encryption, Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Aprill 2011.

[30] D. Tian, Particle Swarm Optimization with Chaotic Maps and Gaussian Mutation for Function Optimization, International Journal of Grid Distribution Computing, Vol. 8, No.4, pp. 123-134, 2015, http://dx.doi.org/10.14257/ijgdc.2015.8.4.12.

[31] H. K. Tai, S. A. Jusoh, W. I. Siu, Chaos-embedded particle swarm optimization approach for protein-ligand docking and virtual screening, Journal of Cheminformatics 10, 2018, https://doi.org/10.1186/s13321-018-0320-9 .