International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 1 370 - 377

Image Encryption using AES Encryption Technique with Bernoulli Chaotic Map

Naresh Mathur
Department of Computer Science Engineering
SIET ,Sikar
Rajasthan, India
nareshmathurer@gmail.com

Abstract

In last few years, the progress in communication technology has seen strong interest in digital picture or image transmission. However, computer processor growth in possessing power and storage illegal access has become easier. Encryption method involves some special mathematical algorithms and keys to transform digital data into cipher text or code before they are transmitted and decrypted method involves the application of mathematical algorithms and keys to obtain the original data from cipher text or code, scientific community have seen strong interest in image transmission. However, illegal image or data access has become more easy and established in wireless and general communication networks. Information privacy becomes a difficult issue. In order to protect, secure your valuable image or data from unauthorized readers, data or image encryption or decryption is essential, furthermore. As such in this paper, AES based on encryption has been proposed for secure image transmission over channels.

1. Background

The majority of the algorithms purposely intended to encrypt digital images have been proposed in the mid-1990s. There are two most important groups of image encryption algorithms:

- Non-chaos selective methods
- Chaos-based choosy or non-selective method

However, nearly all of these algorithms are planned for an explicit image format, also compressed or uncompressed [1]. These are method the offer slight distortion, while offer powerful form of encryption. Most of the algorithms are scalable and have dissimilar mode range from dilapidation to physically powerful encryption. The users are expected to select a method based on its properties, which will be better for image security [2].

Image encryption has application in multimedia system, internet communication medical and military image systems. Every type of multimedia data has its own properties such as strong correlation among pixels and high redundancy [3]. Thus, dissimilar techniques must be used to protect secret image data from unauthorized access.

1.1 Symmetric Key Algorithm

In general, symmetric key algorithms utilize a single, public secret key. The same key is used for both encrypting and decrypting data. There are two types of symmetric-algorithms:

- Block Cipher
- Stream Cipher

A block cipher is used to encrypt a data to produce a cipher data, which transforms a fixed-length of block size into same length-block of cipher text in which a private key and algorithm are applied to the slab of data [5][6].

1.2 Chaos

The next law of thermodynamics state that the measure of disarray of the universe increase over time which is a different way of saying that there is a lot of confusion in our life.

Definition: A dynamical organization describes how time changes and affects a convinced state.

Definition: Determinism is the plan that the whole object is the result of earlier characteristics. These resources can be predicted due to their initial states and actions. The dependence on early

state is very significant in chaos, because the result is mainly dependent on the initial state [7].

Definition: A small uncertain event would eventually overcome any calculation and defeat the accuracy of your guess is known as the butterfly effect.

The butterfly effect result is typically mentioned when the topic of chaos comes up, and its power because it is such an attractive question to ponder. Another thing is that Henri Poincare was the first to detect the possibility of chaos and consider it; Lorenz was the first to work with an example [8]. He was a meteorologist who noticed the uncertainty of climate. Lorenz had a thought to try mathematically and come up with a system that would foresee weather model. While doing this he exposed that the solutions never came to a resting point, but that they would carry on to oscillate in an irregular and periodic fashion. He also messed around with his primary conditions and found that it really affected the result.

1.3 Bernoulli Logistic Map

Bernoulli map is a phenomenon that happen in non-linear definable systems responsive to initial situation and has a pseudo-random behavior. Dynamic-chaotic system in crate of Liapunov exponential equations get together will remain stable in chaos mode [9]. An imperative attribute that has caused this occurrence to get into consideration for cryptographic algorithms is being definable in spite of its pseudo-random performance. Due to pseudo-random activities, the output of the dream system seems random in attacker's sight, while in established view, the system can be defined and decryption is probable. Various cryptographic based on chaos-theory is accessible till now and in ways that are capable of image encryption addition to text encryption. Image encryptions have to have suitable speed for enormous image data ciphering. Text encryption method is not suitable for finish on the image. Almost, we need to broadcast a sensible amount of data, which necessitate a great gap and that in turn involve a big amount of keys[10].

The chaos is a process of exact pseudo-random series created by non-linear dynamics-system. It's responsive to the unique price and non-periodic, non-astringe. Logistic-maps are a characteristic chaotic-map and it's appear is shown as equation.

$$Xn + 1 = bXn\,(1 - Xn)$$

Where $X_n \in [0,1]$, when the worth of restriction b is between(3.569,4), the system has the chaotic properties, and then the series created by logistic-maps are random and dependent on primary value.

2. Arnold Cat Map (ACM)

In the 1960s Vladimir Arnold exposed the ACM, and he used the picture of a cat in his analysis. Previous to stating the description of the ACM, there is little word that requires being distinct and they are torus and stage gap [11][12].

Definition: A torus is the outside of a rotating ring in three dimensional seats, approximately a disengaged alliance that is coplanar to the ring.

Definition: A stage gap is a space in which all possible state of a association are symbolize, where various state are symbolize by one single end in that stage gap.

These are two definitions will help us out really in sympathetic the next one.

Definition: A chaotic map recognized as the ACM is a separate system that stretch and fold the trajectory in phase space, which will be a torus. Mathematically the ACM can define as the following:

Let $X=\begin{bmatrix} x \\ y \end{bmatrix}$ be the n×n matrix, then Arnold cat map transformation is,

$$\Gamma: \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

i.e.) $\Gamma: (x, y) \rightarrow (x + y, x + 2y) \bmod n$

Note: mod is the remainder of $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ and n.

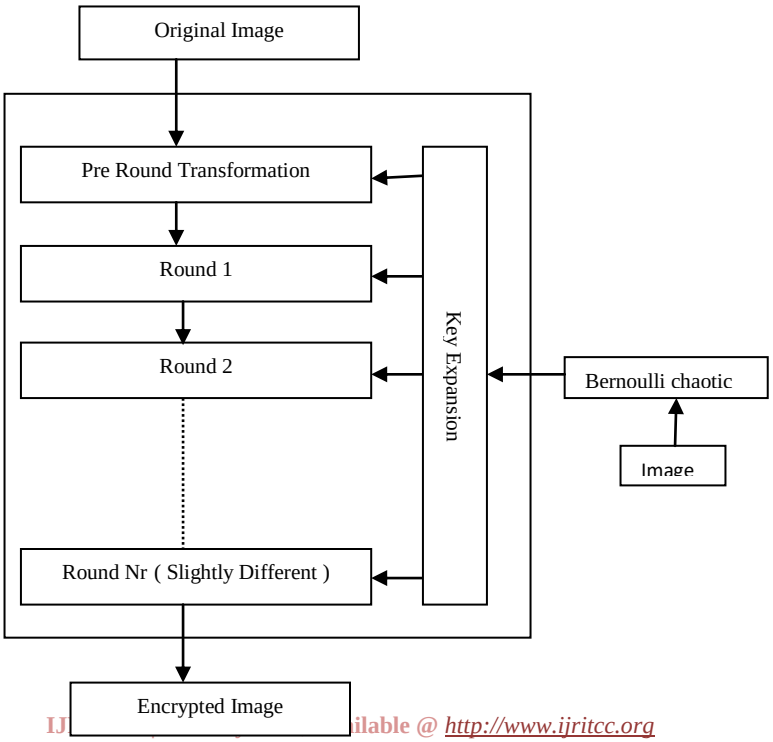
We can also represent this as the system shown below

$$X2 = (2x_1+y_1) \bmod 1$$

$$y_2=(x_1 + y_1) \bmod 1$$

The definition means the Arnold cat map is constantly applying its map to a given i/p and all the iterations moves the pixel values to a unique equivalent point along the same torus. In other words, the Arnold cat map is iterating the picture in the given torus, and all iteration will give us with a new image that has the same dimensions. The iterated images will return to the original image[13]. Since it is a chaotic map, the separate scheme that makes it up, show the dynamics of chaos. The ACM is easy and stylish expression and design of a number of the philosophy of chaos – that is, original order seems that it is an accidental development of a system. Therefore we recognize that the ACM will be unfair by its earlier situation and the output will appear to be accidental.

3. Propose Method



4. Implementation

In this section we evaluate the Bernoulli chaotic map of an image and then use that Bernoulli chaotic image as a key for encryption the real image using advance encryption standard (AES). We make the Bernoulli chaotic image of the main image by using Arnold cat-map alteration. Arnold Cat-map (ACM) change is performed by using this function,

Γ: (x, y) → (2x+y, x+y) mod 1

One of this map's features is that image being randomized by the transformation, other than recurring to its original state after a number of steps. In this paper, we used only one step of the alteration of the image. For an image or picture, the relationship between iterations could be represented as follows:

For n=0: $T^0(x, y)$ = Input Image(x, y)

For n=1: $T^1(x, y) = T^0$ (mod (2x+y,N),mod (x+y, N))

For n=k: $T^k(x, y) = T^{k-1}$(mod (2x+y, N), mod(x+y, N))

For n=m: Output Image(x, y) = $T^m(x, y)$

In this proposed approach we are using only first iteration of the Bernoulli chaotic image of original image of Lena, and this Bernoulli chaotic image treated as the key for encryption of the original image of Lena. Original image of Lena and Bernoulli chaotic image of first iteration of the unique image are shown as below:

Fig1 Main Image

Fig 2 First Iteration of Arnold cat-map of main Image

After receiving the chaotic image of the original image, we require to creating a binary image of the Bernoulli image, this binary conversion of the Bernoulli image will be use as the key for AES to encrypt the original image.

5. Performance Analysis

A good encryption procedure should be robust against all kind of cryptanalytic, arithmetical and brute-force attack. In this section, the security includes statistical analysis, sensitivity analysis, and information entropy analysis and speed performance.

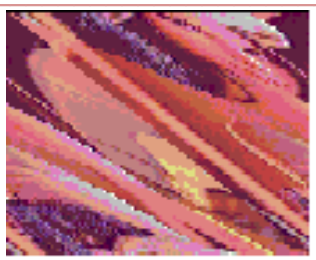
- **Statistical Analysis**

In order to resist statistical attacks, image encryption must possess certain random properties. A detail study has been explored and the results are summarized. The result for lena image as shown in Fig.3

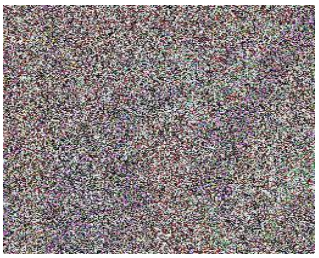
- **Color Histogram**

In Fig. 3 frame (a), (b) and (c) show the histogram of RGB colors for original (Fig.1), frame (e), (f) and (g) show the histogram of the encrypted images (Fig.4) and Fig. 2 shows the first iteration of the chaotic image of the image, which is created by Arnold-Cat-Map (ACM). The figure clearly presents the random-like appearance of the encrypted images.

(a)

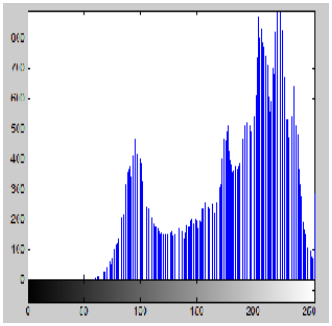


(b)

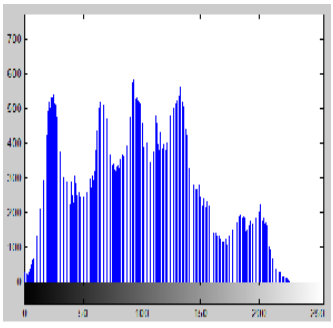


(c)

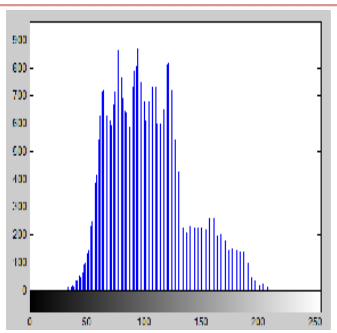
Fig. 3. **(**a) Show the lena Image (b) First Iteration of the ACM of lena image(c) show the encrypted Image of lena



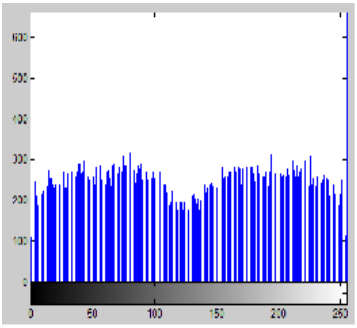
(a)



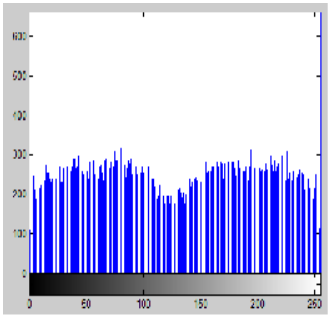
(b)



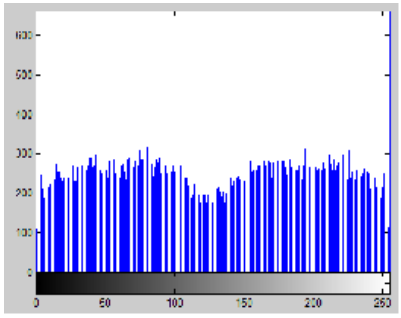
(c)



(d)



(e)



(f)

Fig.4 Frame (a), (b) and (c) are the histogram of the Red Green Blue channels of the image in Fig.1 frame (d), (e) and (f) are the histogram of the Red Green Blue channels of the encrypted image of lena

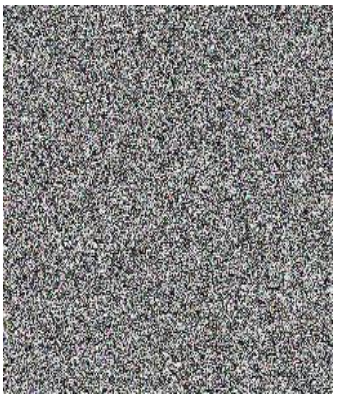
- **Sensitivity Analysis**

An ideal image encryption process must be sensitive with the clandestine key. It income that the alter of a single bit in the secret keys should produce a completely different encrypted image. To perform the sensitivity analysis we use the second iteration of Bernoulli map of the original image of Lena, which makes little difference in the binary value of chaotic map from previously used Bernoulli map. Because of this, the data between the legitimate users require to be protecting before broadcast (transmission) by using encryption methods.

Our algorithm used only replacement approaches to encrypt the image Therefore now we found a new key for encryption of the original image of Lena and now we get the new encrypted image as shown below:

(a)

(b)



(c)

Fig.5 (a) Original image of Lena, (b) encrypted image of the original image of lena by old key, (c) new encrypted image found by the new key

This new encrypted image is completely different from the old encrypted image. The old encrypted image is formed by using first iteration of the Bernoulli map of the original image, while the new encrypted image is found by using 2 iteration of the Bernoulli map of the original image. Thus it will make more difference in the encrypted image by changing the iterations. Therefore, the proposed image encryption process is extremely key sensitive.

- **Information Entropy Analysis**

Information theory is a mathematical theory of data communication and results founded by Shannon. It is well known that the entropy H(m) of a message source m can be calculated as

$$H(m) = \sum_{i=0}^{2^N-1} (p(m_i)) \log(\frac{1}{p(m_i)})$$

Eq. (6.1)

Where N is a number of bits to denote a symbol m_i m. $p(m_i)$ represents the probability of symbol m_i and log( ) stand for the base 2 (two) logarithm so that the entropy is represent in bits. For a truly random source emit 2^N cipher, the entropy is H(m)=N.

If the output of a cipher emits symbols with entropy less than N (entropy < N), there is a certain degree of predictability or inevitability, which intimidate its security. Let us consider the cipher text of Lena's image of size 256x256 encrypted via the proposed scheme. The number of occurrence of each cipher text pixel m_i is recorded and probability of occurrence is calculate for the three image color (R, G and B) components. The entropy for the three image color (R,G,B) components is

$$H_R(m) = \sum_{i=0}^{2^8-1} (p(R_i)) \log(\frac{1}{p(R_i)}) = 7.99938,$$

$$H_G(m) = \sum_{i=0}^{2^8-1} (p(G_i)) \log(\frac{1}{p(G_i)}) = 8.00088,$$

$$H_B(m) = \sum_{i=0}^{2^8-1} (p(B_i)) \log(\frac{1}{p(B_i)}) = 8.00078$$

Eq. (6.2)

With R_i, G_i and B_i are the component of the pixel m_i. The values achieve are very close to the theoretical value N = 08 for the three image color entropy. We can say that information leakage in the encryption method is negligible and the encryption system is secure against the entropy attack.

- **Speed Performance**

Apart from the security consideration, running speed of the algorithm is also good aspect for the encryption method. The

simulator for the planned scheme is implemented using Mat lab 7.0. Performance was measured on 2.40GHz Pentium Core2Duo CPU with 2GB RAM running Windows7. Simulation results give you an idea about the average running time is 0.013163 seconds for encryption and 0.014136 seconds for decryption.

6. Conclusion:

In this paper, a color image encryption scheme is proposed, which is based on ACM of the original-image. The transformation modeled by the ACM and then found a Bernoulli image of the original image, that Bernoulli image is then used for encryption of the original image. As a result the encrypted image demonstrates the randomness of the algorithm. The use of Arnold cat-map increases the confusion of the encrypted image. In fact, analyzing the complete performance result prove the security, robustness of the proposed algorithm. The Security of an image is very different from that of a text-file. Because of its essential characteristics, the encryption speed of the algorithm and algorithm simplicity is generally considered more important. Chaos theory has proved to be an excellent alternative to provide a quick, easy and reliable image encryption scheme that has a high enough degree of security. In this dissertation two chaos based cipher scheme for still image have been analyzed in detail and a new technique combining the advantage of the two systems under analysis have been proposed the scheme has larger key space a new approach to encrypt the image by using a Logistic map with the pixel mapping tables is proposed. In which, the algorithm consists of two replacement methods without any scrambling approach which enhance the execution time of the encryption algorithm. In the first method, we shift each pixel by using a random shifter generated by using the logistic map as a Key1 and modified by using the modulus operation. The resulted image will be mapped by using key2 and modified by using another image; to enhance and increase the uncertainty of the cipher image. However, we shown by experimental results that our algorithm is sensitive to initial conditions (IC) and strong against the brute force attacks. Finally, we found that our algorithm has a highly secure against various types of attacks with the large space of the encryption keys.

- **Future work**

In future, it is intended to speed-up the encryption algorithm through some other Bernoulli map algorithms like as baker's map algorithm other than Arnold cat-map algorithm. These algorithms may maintain the speed performance and randomness of the encryption process and improves the result of encrypted image. If there, we use some more iterations of the real image from Arnold cat-map algorithm then we may get some more diffracted image of the real image, which maintain the security of the original image and the randomness will be maintain of the encrypted image. The project can be widespread in such a way that it may have various future applications. The Project can be extended for encrypting images. Since image comprises was a sequence of Frames. And each frame can be considered as an image. Therefore this algorithm can be extended to encrypt a series of images. The project can also be made more robust and secured by using Arnold Cat map. In the proposed system, a symmetric key is used for encrypting the images.

Reference

[1] Yu, X. Y., J. Zhang, H. E. Ren, G. S. Xu, and X. Y. Luo, "Chaotic image scrambling algorithm based on S-DES", *In Journal of Physics: Conference Series*, vol.-48, no.-1, pp. 349, 2006.

[2] Jiri Giesl Mao, Yaobin, Guanrong Chen, and Shiguo Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps", *International Journal of Bifurcation and Chaos* vol.-14, no.-10 pp. 3613-3624, 2004.

[3] Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud, "Image encryption using chaotic logistic map", *Image and Vision Computing* vol.-24, no.-9, pp. 926-934. 2006.

[4] Salleh, Mazleena, Subariah Ibrahim, and Ismail Fauzi Isnin, "Image encryption algorithm based on chaotic mapping", Jurnal Teknologi, vol.-39, no.-1, pp. 1-12, 2012.

[5] Li, Ping, etal, "A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map", Physics Letters A 349.6, pp. 467-473, 2006.

[6] Wong, Kwok-Wo, Bernie Sin-Hung Kwok, and Wing-Shing Law, "A fast image encryption scheme based on chaotic standard map", Physics Letters A 372, no.-15 pp. 2645-2652, 2008.

[7] Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I& Shore, K. A. (2005) "Chaos-based communications at high bit rates using commercial fibre-optic links. Nature", 438(7066), 343-346.

[8] Salleh, Mazleena, Subariah Ibrahim, and Ismail Fauzi Isnin, "Enhanced chaotic image encryption algorithm based on Baker's map", *In Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*, vol.-2, pp. II-508, 2003.

[9] Krikor, Lala, Sami Baba, Thawar Arif, and Zyad Shaaban, "Image encryption using DCT and stream cipher", *European Journal of Scientific Research*, vol.-32, no.-1, pp. 47-57, 2009.

[10] Gao, Haojiang, Yisheng Zhang, Shuyun Liang, and Dequn Li, "A new chaotic algorithm for image encryption", Chaos, Solitons & Fractals, vol.-29, no.-2, pp. 393-399, 2006.

[11] Mao, Yaobin, Guanrong Chen, and Shiguo Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps", *International Journal of Bifurcation and Chaos*, vol.-14, no.-10, pp. 3613-3624, 2004.

[12] Kumar, Gelli MBSS, and V. Chandrasekaran, "A Generic Framework for Robust Image Encryption Using Multiple Chaotic Flows", *International journal of computational cognition (http://www. ijcc. Us,)* vol.-8, no.-3, pp.13, 2010.

[13] Awad, Abir, and Abdelhakim Saadane, "New chaotic permutation methods for image encryption", IAENG Int. J. Comput. Sci, vol.-37, no.-4, 2010.

[14] Yoon, Ji Won, and Hyoungshick Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps", *Communications in Nonlinear Science and Numerical Simulation*, vol.-15, no.-12, pp. 3998-4006, 2010.

[15] Alvarez, Gonzalo, and Shujun Li, "Some basic cryptographic requirements for chaos-based cryptosystems", *International Journal of Bifurcation and Chaos*, vol.-16, no.-08, pp. 2129-2151, 2006.

[16] Scharinger J., "Fast encryption of image data using chaotic kolmogorov flows", J. Electron Imageing, vol.-7, pp. 318-325, 1998.

[17] Fridrich J., "Symmetric ciphers based on two-dimensional chaotic maps", J. Bifurcat Chaos, vol.- 8, pp. 1259-84, 1998.

[18] Li S J, Zheng X, Mou X and Cai Y, "Chaotic encryption scheme for real-time digital video Proc SPIE on Electronic Imaging", 4666 149-166, 2002.

[19] Lu J and Chen G R, "A new chaotic attractor coined J. Bifurcation and Chaos", vol.-12, pp. 659-661, 2002.

[20] Chen G R, Mao Y B and Chui C KA, "Symmetric image encryption scheme based on 3D chaotic cat maps", J.Chao, Solitons and Fractals, vol.-21, pp. 749-761, 2004.