International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Securing Digital Image using Chaotic-Based Cryptosystem

Zinabu Haile Abirha, Eyerusalem Dagnew Gebru

Abstract*: As the unfold boom of Internet get entry to the need for multimedia specifically digital images are widely applicable in various areas such as military, medical, science, education, advertising, entertainment and many others. As human beings around the world exchange these digital images assuring the privacy and reliability of images has turn out to be a principal concern. Thus ciphering the image comes into account. The relationship between the pixel values of neighboring pixels of a plain digital image is strong. The proposed cryptosystem breaks the relationship of neighboring pixel values by altering its position with the use of Arnold cat map equation. Then the shuffled image is diffused using a symmetric keys to yield an encrypted image. The experimental result shows that our cryptosystem effectively cipher/decipher the digital image with external secret key. The experimental result of the proposed cryptosystem was done using MATLAB R2018a and shows it is capable of producing an encrypted image with extremely low relationship coefficients of neighboring pixels. We also found that it is very sensitive to any input key and parameters change. Consequently the proposed cryptosystem has strong encryption quality and invulnerable way for a colored image. Considering the security necessities, this work can have a focus in securing medical end results, country wide secrets and plenty of others which are exchanged over the Internet.

Keywords: *Cryptography, Confusion, Diffusion, Image, Arnold cat map, Chaos.*

I. INTRODUCTION

Multimedia images are transmitted and kept in storage intently over the Internet. The protection of these digital images in offline storage as well as in the course of transmission is a major hassle in our day today activities.

In latest years, with the unfold growth in statistics and communication technologies, protecting the delivered information from attackers over the worldwide community turns into a vital difficulty.

In cryptography, encryption is that the process of converting a given data using an algorithm to form unrecognized to everyone except those having the knowledge about algorithm and therefore the secret key used. Cryptography has begun starting from the time of classical ciphers like Caesar to contemporary day cipher and public key system like Diffie-Hellman, RSA.

These days cryptography involves the use of superior mathematical processes in the course of encryption and decryption processes, therefore the cipher algorithms are turning into greater complicated daily.

In cryptography, digital computing been utilized to a specific kinds of digital file codecs like text, pictures and videos. Numerous image encryption algorithms had been advanced and over the previous years. However, most of the recognized text content encryption techniques, like DES, AES and RSA are observed ineffective for image cryptosystem. This is due to the processing overhead ensuring from massive statistics size of the digital image and the relationship amongst the image pixels [1], [10], [11].

Thus, we propose an image primarily based encryption method by developing a cipher algorithm for image of size n*n by the usage of Arnold's cat map as pixel permutation and XOR operation on pixel values the usage of external secret keys as diffusion process.

II. CHAOS

Chaos is phenomena governed by deterministic non-linear systems that show severe sensitivity to the preliminary conditions given as input and have widely random behavior [2], [3]. Chaotic structures have a variety of essential characteristics, such as sensitive to the preliminary stipulations and system parameters, non-periodicity, and pseudorandom property, etc. These characteristics results the chaotic system compulsory condition for confusion and diffusion in the experience of cryptography [1], [4], [9].

III. RELATED WORK

To insure the privacy and protection of images several image encryption schemes counseled in this section.

In [2], an image encryption system is developed on the foundation of Arnold's Cat map to change the positions of pixels and chaotic map is used to produce pseudorandom images for substitution. El-Sayed and Khaled A. advocates an encryption system based totally on chaotic maps and genetic operators[5].In [6], Abdurrahman proposed color image encryption the use of random image key generated and XOR operation. In [7], proposed encryption scheme make use of one tent map to generate a pseudorandom sequence and then shift the bits of the expanding 0-1 image circularly to be able to shuffle the image gray values.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Zinabu Haile Abirha*, Faculty of Computing Technology, Aksum Institute of Technology, Aksum, Ethiopia. Email: zinabuscholar@gmail.com
Eyerusalem Dagnew Gebru, Faculty of Computing Technology, Aksum Institute of Technology, Aksum, Ethiopia. Email: jerrydg21@gmail.com

To make the encryption generalized Arnold maps and Bernoulli shift maps are applied to supply two pseudorandom gray value sequences after which diffuse the gray values bi-directionally.

In [8], suggest an image encryption primarily based on the chaotic permutation more than one round circular shrinking and expanding.

In [10], Fu and Zhu proposed an image cryptosystem the use of logistic maps for permutation and circular bit-shift technique for confusion and diffusion. Wei-bin and xin proposed an algorithm that makes uses Arnold's cat map to shuffle the pixels of the original image and one dimensional Henon's chaotic map to exchange the shuffled pixels with the aid of XOR operation [12]. In [13], an encryption system based totally on 3D Lorentz system is developed to enhance the protection and overall performance of an encryption over the traditional 1D chaos based.

IV. PROPOSED CRYPTOSYSTEM

The proposed cryptosystem consists of two phases: key setup and encryption algorithm. Arnold's cat map is employed in confusion stage.

A plain digital image is given as a source to the cryptosystem from file which it will be ciphered and a number of iteration ***R***, ***a*** and ***b*** as parameters and external secret key.

A. Key set up

In this proposed scheme, we use a 120-bit external secret key as an input. Based on the secret key we have to generated three separate keys out of the 120-bit to be applied to the R, G, B pixel value during encryption.

Now, we will obtain the three keys, keyR, keyG, and keyB from the external secret key based on the following steps:

***Step 1*:** The external 120-bit key long is divided into blocks of 8-bit length.

$$Key = K_1 K_2 K_3 ... K_{15} \quad \text{.....(1)}$$

Where each K_i's is the secret key represented in its ASCII mode.

Step 2: The external secret key is mapped into three blocks of each 40-bit key represented as ASCII mode, and applied to diffuse the RGB pixel value of the shuffled image.

$$Block1 : K_1, K_2, K_3, K_4, K_5$$

$$Block2 : K_6, K_7, K_8, K_9, K_{10} \quad \text{And}$$

$$Block3 : K_{11}, K_{12}, K_{13}, K_{14}, K_{15}$$

We compute the sum of each block as:

$$\boldsymbol{Block}_i = \sum_{j=1}^{j=5} K_j \quad \text{MOD 256} \quad \text{..... (2)}$$

Where i=1, 2, 3 , and $\boldsymbol{Block}_i$'s represents keyR, keyG and keyB respectively.

B. Encryption Algorithm

The general block diagram of the proposed encryption scheme is shown in Fig. 1. The input to the cryptosystem is the plain image which it will be ciphered, the number of iteration ***R***, ***a*** and ***b*** parameters for Arnold's cat map and external 120-bit secret key. The encryption system consists of two stages the so-called confusion and diffusion.

The detail steps in the encryption process are depicted as follow:

Step 1: Read Image to be encrypted from file

Step 2: Read 120-bit secret key

Step 3: Arrange 3 keys to diffuse the RGB pixel based on key setup using (1) and (2)

Step 4: Permutation/Confusion

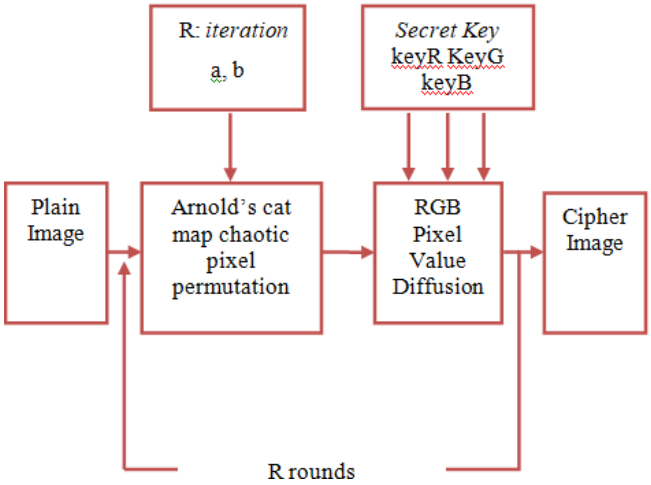


Fig. 1. General block diagram of cryptosystem

In confusion stage the R, G, B pixel values are permuted where the position of each pixels value of the R, G, B is distributed over the entire digital image without changing the original value of R, G, B pixels and the image becomes unrecognizable.

The input to the confusion stage is the normal encipher image and the number of iteration ***R***, **a**, ***b*** as a parameter. Arnold's cat map is used for confusion and iterated ***R*** rounds based on the input iteration, where the new location is a function of the old ones as in (3):

$$\begin{bmatrix} Xnew \\ Ynew \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} MOD(N) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \text{..... (3)}$$

Where ***a*** and ***b*** are positive integers as input parameters and N is the size of the original image, original position of the image pixel before scrambled as ***X***,***Y*** and ***Xnew***, ***Ynew*** are new location of the pixel right after scrambled.

Step 5: Substitution/Diffusion

In this step, the original R, G, B pixel values are altered primarily based on (4), (5) and (6) using XOR operation.

We diffuse each R, G, and B pixel to get the cipher R, G and B pixel value using XOR operation as follow:

$$\boldsymbol{CipherB}(i,j) = \text{pixelR}(i,j) \oplus \text{KeyR} \quad \text{..(4)}$$

$$\boldsymbol{CipherR}(i,j) = \text{pixelG}(i,j) \oplus \text{KeyG} \quad \text{.....(5)}$$

$$\boldsymbol{CipherG}(i,j) = \text{pixelB}(i,j) \oplus \text{KeyB} \quad \text{..(6)}$$

V. EXPERIMENTS AND SECURITY EVALUATION

In this section, we have tested different experimental effect to show the efficiency of the newly proposed cryptosystem. To conduct our test we had written a code in MATLAB R2018a and the experimental results was once performed based totally on numerous standard images. Thus let us focus on the following known encryption quality metrics:

A. Correlation Coefficient

The correlation coefficient is used to evaluate the encryption quality of our proposed cryptosystem and can be calculated using (7).

$$C.C = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum x_j^2 - (\sum_{j=1}^{N} x_j)^2) \times (N\sum y_j^2 - (\sum_{j=1}^{N} y_j)^2)}}$$

…… (7)

Where ***x*** and ***y*** are the original and encrypted digital images pixel values.

Table- I Correlation coefficients between several plain and Corresponding Cipher Images

Image Name	Image Size (pixel)	Correlation Coefficient
Fruits	512x512	-9.0109e-04
Lena	512x512	6.1100e-04
Peppers	512x512	-0.0016
Fruits	256x256	2.8336e-04
Lena	256x256	-6.5908e-04
Peppers	256x256	0.0016

The calculated correlation values after generating cipher image using the key "***bd7c4f334b61432f4d54226c505e21***" and **R**=20, **a**=2, **b**=0 as parameters is indicated in Table I. This shows the correlation coefficient of all input images are very low and approaches to zero. This proves the proposed cryptosystem is more tightly closed system.

B. Key Space Analysis

The key space provides complete wide variety of distinct keys that are going to be used in the cryptographic system [8]. The secret keys of our proposed cryptosystem is (***R, a, b, K***) where ***R*** ε ***3*N***, ***a*** and ***b*** are positive integers between 0-255, and K is 120-bit external secret key. If we consider the secret key "***K***" only, we have 2^{120} (≈1.33 x 10^{36}) different combination of secret key and a digital image encrypted with such a large key space is appropriate for reliable encryption applications and can resist all possible brute force attacks.

C. Key Sensitivity Test

Any digital image cryptosystem ought to be sensitive with the applied secret key. That is change a single bit in any of its secret key should yield absolutely different encrypted image. To show the key sensitivity test, we carried out digital image encryption with two different secret keys that only differ in a single bit in the right most list significant bit. The two keys ***key1*** and ***key2*** in hexadecimal are "***7d7c4f334b61432f4d54226c505e2f***" and "***7d7c4f334b61432f4d54226c505e21***" keeping all the parameters constant for both these keys. We cannot easily recognize the distinction of the generated cipher image with naked eye. Thus, we examine using the correlation coefficient (7). The cipher images based on these applied secret keys, for the original digital image in Fig. 2 A, are shown in Fig. 2 B and Fig. 2 C respectively. Furthermore, we have got performed for same in lena and peppers images with the above parameters and we observed the end result as in Table II.

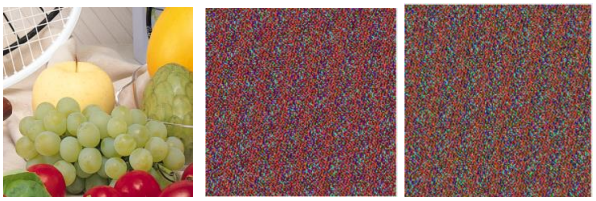


Fig. 2. (A) (B) (C)

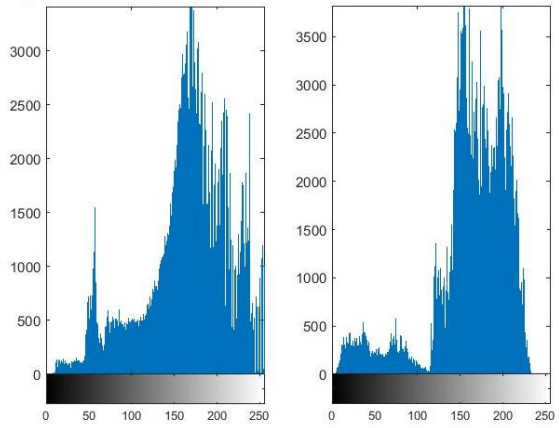
Table II Correlation Coefficient between Plain Image and Cipher Image under Key1 and Key2

Image Name	Image Size (pixel)	Correlation Coefficient	
		First key	Second key
fruits	512x512	3.9409e-04	0.0014
lena	512x512	-1.6893e-04	-3.5688e-04
peppers	512x512	0.0021	0.0025

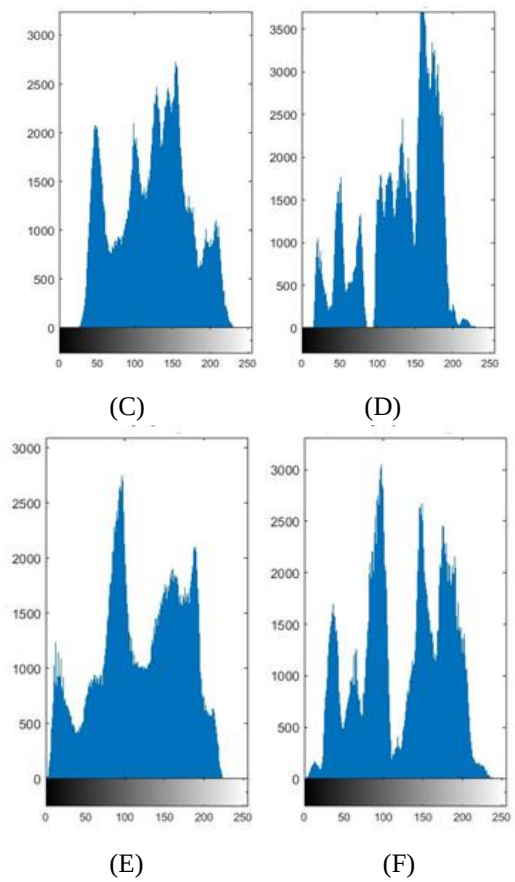
VI. RESULT

To reveal a few experimental analysis, we recall the subsequent further to the experimental and security evaluation in **V**.

A. Histogram Analysis: If a designed image cryptanalysis algorithm can generate a uniform distribution of the pixels in the ciphered images, then it is able to successfully withstand the histogram attack. We have plotted the histogram of plain versus cipher image of fruit, lena and peppers all with image size 512x512 in Fig. 3 respectively.



(A) (B)



(C) (D)

(E) (F)

Fig. 3. Histogram analysis: (A) fruit plain image; (B) fruit cipher image; (C) Lena plain image; (D) Lena cipher image; (E) pepper plain image; (F) : pepper cipher image

In Fig. 3, all the plotted histogram of plain versus ciphered images of every type is unique; this indicates that an illegal statistical attack will no longer affect our proposed algorithm.

B. Plaintext Sensitivity Analysis: Table III. Suggests the result of plain image sensitivity analysis which we can show using the NPCR (Number of Pixel Change Rate)is over 99% and UACI(Unified Average Intensity)is over 38%. This suggests that our proposed cryptanalysis is extremely sensitive to plain image, consequently, can correctly face up to chosen-plain attack.

Table III NPCR and UACI

Image Name	Image Size (pixel)	NPCR	UACI
fruits	512x512	0.9965	3.8147e-04
lena	512x512	0.9966	3.8147e-04
peppers	512x512	0.9974	3.8147e-04

VII. CONCLUSION

Highly sensitive digital images like medical end result, national secrets and many others which are exchanged over the Internet are liable to attackers. Thereby, assuring the privacy and reliability of images has turn out to be a principal concern, thus, we brought a technique for encrypting a color digital image primarily based on a chaos. The encryption algorithm use Arnold's cat map for pixel shuffling and XOR operation using external input secret keys to modify the pixel values. Here, 120-bit external input secret key is mapped into three different keys KeyR, KeyG, and KeyB in order to XOR the RGB pixel values. We carried out a number of experiments using MATLAB R2018a and the result shows that the proposed approach is able to generating a cipher image with extraordinarily low correlation coefficients of neighboring pixels. We also found that it is easily sensitive to any input key and parameters change even if we can change a single bit of the key. Furthermore, from the result analysis we conclude that the cryptosystem can correctly face up both statistical and chosen-plain attack. As a result our proposed cryptosystem has strong encryption quality and invulnerable way for colored-image encryption.

REFERENCES

1. G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," vol. 21, pp. 749–761, 2004.
2. I. S. I. Abuhaiba, H. M. Abuthraya, H. B. Hubboub, and R. A. Salamah, "Image Encryption Using Chaotic Map and Block Chaining," no. July, pp. 19–26, 2012.
3. M. Ahmad, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping," vol. 2, no. 1, pp. 46–50, 2009.
4. O. M. A. Zaid, N. A. El-fishawy, and E. M. Nigm, "CryptosystemAlgorithm Based on Chaotic Systems for Encrypting Colored Images," vol. 10, no. 4, pp. 215–224, 2013.
5. S. Arabia, "An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators," no. c, pp. 92–97, 2011.
6. A. D. Khalaf, "Fast Image Encryption based on Random Image Key," vol. 134, no. 3, pp. 35–43, 2016.
7. R. Ye, "An Image Encryption Scheme Based on Bit Circular Shift and Bi-directional Diffusion," no. December 2013, pp. 82–92, 2014.
8. Y. Suryanto and K. Ramli, "A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding," vol. 7, no. 4, pp. 697–713, 2016.
9. Zhang LH, Liao XF, Wang XB, "An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, Vol. 24, 2005; pp. 759–765
10. C. Fu and Z. Zhu, "A chaotic image encryption scheme based on circular bit shift method," in Proc. of the 9th Int. Conf. for Young Computer Scientists, (ICYCS 2008), Nov. 2008, pp. 3057-3061.
11. G.M.B.S.S. Kumar and V. Chandrasekaran, "A novel image encryption scheme using Lorenz attractor," in Proc. of the 4th IEEE Conf. on Industrial Electronics and Applications, (ICIEA 2009), May, 2009, pp. 3662-3666.
12. C. Wei-Bin and Z. Xin, "Image encryption algorithm based on Henon chaotic system," in Proc. of the Int. Conf. on Image Analysis and Signal Proc., (IASP 2009), April 2009, pp. 94-97.
13. Chong Fu, Zhen-chuan Zhang, Ying-yu Cao, "An improved image encryption algorithm based on chaotic maps," in Proc. of the 3rd Int. Conf. on Natural Computation, (ICNC 2007), 2007

AUTHORS PROFILE

Zinabu Haile Abirha, is a lecturer in the faculty of Computing Technology, Aksum Institute of Technology, Ethiopia. He received his MTech (CSE) from Indian Institute of Technology Guwahati (IITG) in 2014. He received his Bachelor of Science in Computer Science from Addis Ababa University, Ethiopia in 2011.

Eyerusalem Dagnew Gebru, is a lecturer in the faculty of Computing Technology, Aksum Institute of Technology, Ethiopia. She is currently Library and Documentation Directorate Director. She received her MTech (CSE) from Indian Institute of Technology Guwahati (IITG) in 2015. She received her Bachelor of Science in Computer Science from Arbaminch University, Ethiopia in 2012.