NEW ALGORITHM FOR FEATURE LEARNING ON ENCRYPTED IMAGES

Onyecherelam Henry Agbaeze,

***Abstract*— In this paper, I present a new learning algorithm for extracting translation invariant features for image classification. Using the golden ratio and a new filtering method that collapses the pixel output from the convolution layer into a learned feature representation, keeping its statistical properties intact In this paper, I present a new learning algorithm for extracting translation invariant features for image classification. Using the golden ratio and a new filtering method that collapses the pixel output from the convolution layer into a learned feature representation, keeping its statistical properties intact**

I. KEYWORDS

Convolution, Pooling, classification, Translation invariant

II. INTRODUCTION

So many learning algorithms have been proposed to address the issue of feature learning on images. Many techniques like filtering max-pooling, statistical and even transformational techniques have been utilized to achieve good results in image classification and segmentation tasks. There are still a few challenges with current methods used for image classification.For an algorithm to learn representations in a pixel, the characteristics of the algorithm must be such that the location of the pixel does not affect the general classification of the image. Both convolution and max-pooling are the most wildly used method for feature extraction[2]. However the performance of both Max-pooling and average pooling has been highly critizied[5]. Researchers now seek a more intuitive approach to feature learning during image recognition

In other to understand Chaos-based image encryption algorithms, it is essential to fully grasp the fundamental theory of Chaos and how it is used for image encryption. Chaos theory states that small changes in initial conditions can lead to vast differences in the outcome. Chaos theory is used to describe systems that are deterministic but inherently unpredictable [13]. The behavior of specific nonlinear dynamic systems whose dynamics are very sensitive to initial conditions. Chaos theory helps us to define a chaotic map is which is used for image encryption. This mapping is merely a function that is characterized by chaotic behavior. Chaotic maps are represented by a formula hence they are deterministic. They are also sensitive to initial values which makes them nonlinear and unpredictable. Chaotic maps appear random and formless but beneath this half haphazardness, it has a visible order and pattern. It is this property that is harnessed for image encryption.

A. *Algorithm Process*

This algorithm takes in greyscale images (images with one channel) as input and uses a single encryption key to carry out its operation. The encryption key or the secret key acts as a mask used to protect the image. The Logistic map function is used to generate the key used for the encryption (alpha)[11]

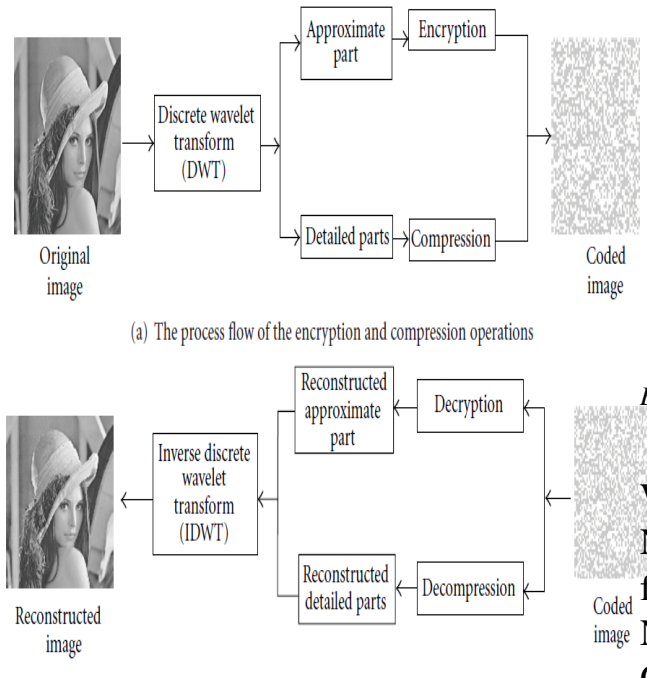
$$x_{n+1} = \alpha x_n(1 - x_n) \tag{1}$$

$$x_{n=0} = x_0 \tag{2}$$

III. New Algorithm Approach

The Logistic Map function generates three keys which may be used independently or as a combination. The first key is the external control parameter (alpha), the second is the initial state (xo) and the last is the number of rounds[6]. These three values as input to the logistic map function which makes it useful as a pseudo-random generator. The length of this PRG ranges from We can generate a pseudo-random number. The length of this PRG varies from 0 to 1, so we can multiply it by 255 and round it to the nearest integer. This integer is converted to an 8-bit binary number.

Fig. 1. Process Flow of Algorithm



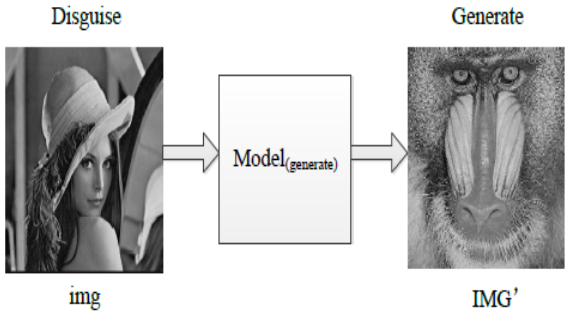
(a) The process flow of the encryption and compression operations

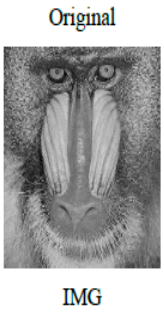
(b) The steps of decryption and decompression taken to reconstruct the image

A. *Image Disguise Based on a Generative Model.*

The output of an encrypted image is usually a random looking image whose coordinate values look ”shuffled.” in the spatial domain. Even though there may be no visible clue to what permutation or encryption scheme was used to encrypt the image, the image itself is a visual clue that the image is a cipher. Image disguise based on a generative model tries to implement an encryption algorithm that produces an image the look ’sensible’ in other to confuse an onlooking attacker that is the image is a cipher[9].

Fig. 2. Process Flow of Algorithm





B. *Encryption Approach*

This encryption method uses the Wasserstine Generative Adversarial Networks (GAN)[5] which is an improved form of the Generative Adversarial Network. GAN was introduced by Ian Goodfellow in 2014. GAN produces a new training idea, in this case an image and has hastened many other works[9]. The WGAN model is applied to generate the handwritten word by feeding the random noise z, but when the random noise z is changed to a meaning-normal image which is independent of the original image, the model can still generate IMG0 visually

the same as original image IMG. These several images taken from the standard set of images were evaluated in the paper, they are Lena, Baboon, Cameraman and Pepper, and they have the same size as 256 by 256. The feed is a meaning-normal and independent image and is trained using a WGAN, then it can generate the visually same as the original image with the disguise image and the trained generator[10]

Fig. 3. Result Chart

Algorithm	Time (in seconds)
Bourbakis(SCAN patterns)	2.54
Mitra (CPT)	1.82
Proposed Algorithm	1.41

Table 3: Computational Time for 1024x1024 Lena Image.

IV. Image Encryption Based on Rubik's Cube Algorithm

This algorithm works using the Rubiks cube algorithm. The number of rows and columns of the image is first computed. Two secrete keys are generated whose length is equal to the length of the rows and columns of the image[12]. Next image pixels are then scrambled using the Rubiks cube principle. After this step, the current pixel values are XORed with the generated keys. The operation for this algorithm is described in the diagram bellow[14].

V. Advantages of New Algorithm

There are a few advantages in using this method for feature learning. One is that the algorithm captures the underpinning statistical variance among the pixels during pooling. The algorithm also takes into account

Fig. 4. Process implimentation

Figure 2(a): Mountains

Figure 2(b): Encrypted Mountain

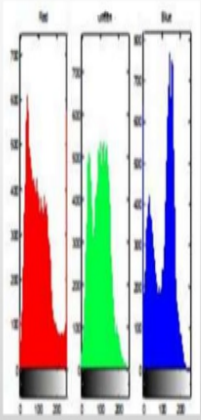


Figure 2(c): Histogram of Mountain

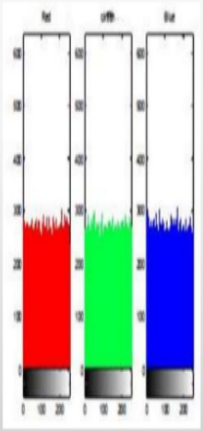


Figure 2(d): Histogram of Encrypted Mountain

the orientation of the image. As long as the shape of the image remains somewhat the same, the translational variate of the image is kept and used while training a neural network.

VI. Disadvantage of New Algorithm

One disadvantage of this algorithm is that it works on only grayscale images. A more robust way to use this algorithm on images with more that one channel is yet to developed. This makes the application areas of the algorithm limited to only specific domains. This algorithm also works on fixed size input of images of 64x64. It is still not certain if the algorithm still works if is run on scaled images. The proof of this is somewhat convoluted. Another disadvantage may arise in the interpretation of the probabilistic features of the images.

VII. Conclusion

This work focuses on grayscale images. More work has to be done in the future to apply this algorithm to higher dimension images with multiple channels. Also, new image processing algorithms used in artificial neural networks called capsule networks[5] can also be used together with this algorithm to provide higher performance.

VIII. Future Work

This work focuses on grayscale images. More work has to be done in the future to apply this algorithm to higher dimension images with multiple channels. Also, new image processing algorithms used in artificial neural networks called capsule networks[5] can also be used together with this algorithm to provide higher performance. Scaling the input image before applying the algorithm does not seem to work well. More work has to be done in this area to improve the performance of the algorithm

References

[1] L. Bao and Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences, vol. 324, pp. 197207, 2015.

[2] T. Filler and J. J. Fridrich, Gibbs construction in steganography, IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 705720, 2010.

[3]] V. Holub and J. Fridrich, Designing steganographic distortion using directional filters, in IEEE International Workshop on Information Forensics and Security, 2013, pp. 234239.

[4] V. Holub, J. Fridrich, and T. Denemark, Universal distortion function for steganography in an arbitrary domain, Eurasip Journal on Information Security, vol. 2014, no. 1, p. 1, 2014.

[5] D. Hou, W. Zhang, and N. Yu, Image camouflage by reversible image transformation. Academic Press, Inc., 2016.

[6]] F. Hu, C. Pu, H. Gao, M. Tang, and L. Li, An image compression and encryption scheme based on deep learning, 2016.

[7] Smolensky, Information processing in dynamical systems: foundations of harmony theory, 1986, pp. 194281. [8] R. Salakhutdinov and G. Hinton, Deep boltzmann machines, Journal of Machine Learning Research, vol. 5, no. 2, pp. 1967 2006, 2009.

[8] R. Pfarrhofer and A. Uh, Selective image encryption using JBIG, in Proceedings of the Communications and Multimedia Security (CMS 05), pp. 98107, September 2005.

[9] T. Kunkelmann, Applying encryption to video communication, in Proceedings of the Multimedia and Security Workshop at (ACMMultimedia 98), pp. 4147, England, UK, September 1998.

[10] L. Qiao and K. Nahrstedt, Comparison of mpeg encryption algorithms, Computers and Graphics, vol. 22, no. 4, pp. 437 448, 1998.

[11] B. Bhargava, C. Shi, and S. Y.Wang, MPEG video encryption algorithms, Multimedia Tools and Applications, vol. 24, no. 1, pp. 5779, 2004.

[12] J. But, Limitations of existing MPEG-1 ciphers for streaming video, Tech. Rep. CAIA 040429A, Swinburne University, Melbourne, Australia, April 2004.

[13] A. Pommer and A. Uhl, Selective encryption of waveletpacket encoded image data: efficiency and security, Multimedia Systems, vol. 9, no. 3, pp. 279287, 2003.

[14] H. Cheng and X. Li, Partial encryption of compressed images and videos, IEEE Transactions on Signal Processing, vol. 48, no. 8, pp. 24392451, 2000.

[15] X. Li, J. Knipe, and H. Cheng, Image compression and encryption using tree structures, Pattern Recognition Letters, vol. 18, no. 11-13, pp. 12531259, 1997.