International Journal of Computer Applications Technology and Research
Volume 6–Issue 1, 66-69, 2017, ISSN:-2319–8656

Image Encryption and DWT Based Copy-move Image Forgery Detection

Gawtham Srinivasan R
Dr. Mahalingam College of Engineering &Technology
Pollachi, India

Lokesh K
Dr. Mahalingam College of Engineering &Technology
Pollachi, India

Abstract: In the present world, digital images are one of the main carrier of information. However the digital images are easily getting tampered due to the availability of image editing software such as adobe Photoshop and so on. It is possible to remove important features or information from an image without leaving any traces. Therefore as a solution to the above mentioned problem, we are proposing a unique solution to detect the copy-move image forgery. In proposed scheme the image is encrypted at client side and it will be decrypted at receiver end for authentication purpose. The image is segmented into non-overlapping blocks .Then statistical features are extracted and reduced to facilitate the measurement of similarities. Finally the Euclidian distance has been calculated and duplicate image blocks are identified after post processing. Experiments results demonstrate that our proposed method is able to detect multiple examples of copy-move image forgery and precisely locate the duplicated regions. We are currently working to improve detection in overlapping blocks.

1. INTRODUCTION

Digital images are subjected to various kinds of attacks and damages due to the prevalence of various image editing software such as adobe photo shop etc. One of the most important type of image manipulation is copy move forgery. In this type, a portion of the image is copied and placed in a different location. We devised a method to identify the copy move forgery using some statistical features.

2. RELATED WORKS

Most methods used in the detection of copy–move forgery can be categorized as either block-based methods or key point based methods. The first such method was proposed by Fridrich using a block matching detection scheme based on discrete cosine transform (DCT). Popescu and Farid proposed a copy–move forgery detection method, which differs in its representation of overlapping image blocks using principal component analysis (PCA) instead of DCT. Some approaches involve the extraction of points of interest using a scale-invariant feature transform (SIFT) capable of detecting and describing clusters of points belonging to cloned areas.

SIFT-based schemes are still limited in their detection performance due to the fact that it is only possible to extract key points from specific locations in an image. In addition, these methods are susceptible to a number of post-processing operations, such as blurring and flipping.

However, some key points of duplicate regions cannot be identified using key point based algorithms and copied regions with little textural structure may be missed entirely.

3. COPY MOVE FORGERY DETECTION

The social media, news sources mainly depends on the digital images to represent the truth of the stories; however, digital images processing tools readily available to make the tampered images for malicious reasons. Various methods have been developed to counter tampering and forgery in order to ensure the authenticity of images. Current forgery detection methods can be categorized as active and passive (blind). Most active methods are based on digital signatures and watermarking; however, this requires that data be pre-processed, which can be troublesome. Passive methods are used to analyse images without using a priori information (such as embedded watermarks or signatures), such that a blind decision must be made regarding whether images have been tampered with. Most passive techniques are based on supervised learning through the extraction of specific features to differentiate the original image from tampered versions. The practicality and wide applicability of passive methods have made them a popular topic of research.

Copy–move is the most common form of digital image forgery, in which a portion of an image is copied and pasted into another portion of the same image to conceal something or duplicate elements. The wide availability of image processing software has made it easy to perform copy–move operations. The region altered by copy–move forgery is often almost imperceptible by the human eye; therefore, detecting evidence of these actions is an important issue in image forensics. This paper presents a robust algorithm for the detection of copy–move forgery based on the histogram of oriented gradients (HOG). The performance of the proposed method is compared with existing methods with regard to detection accuracy and computational complexity.

4. ENCRYPTION AND DECRYPTION

Nowadays internet is used for faster transmission of large volume of important and valuable data, since internet has many points of attack, it is vulnerable to many kinds of attack, so this information need to be protected from unauthorized access, To protect data from unauthorized access there are many data protection techniques like Nulling Out, Masking Data, Watermarking, Encryption etc. are implemented.
Data Encryption is one of the widely used techniques for data protection. In Data Encryption, data is converted from its

original to other form so that information cannot be accessed from the data without decrypting the data i.e. the reverse process of encryption.

The original data is usually referred as plain data and the converted form is called cipher data. Encryption can be defined as the art of converting data into coded form which can be decoded by intended receiver only who possess knowledge about the decryption of the ciphered data. Encryption can be applied to text, image and video for data protection.

In proposed work we use two simple techniques namely:

- Permutation.
- Substitution.

In Permutation pixels of images are relocated to different location in the image using the chaotic map sequence.

In Substitution pixels of the original image are multiplied with the key image pixels.

We combine both substitution and permutation to form an encrypted image. This encrypted image is used for authentication.

At the receiver end, Receivers are provided with the key and the encrypted image. The receiver decrypts the image and process the image for the identification of copy move forgery.

Decryption is simply the reverse process of encryption.

4.1 Chaotic Sequence

Pseudo Random Number Generators (PRNGs) are widely used in many applications, such as numerical analysis, probabilistic algorithms, secure communications, integrated circuit testing, computer games and cryptography. The quality of randomness is usually the main criterion to distinguish the different PRNGs. Besides the quality of randomness, implementation cost and throughput are also important factors to evaluate the effectiveness of the PRNGs in applications, such as modern communications, image encryption, video encryption and sensor networks, and so on.

Chaos has widely been used in cryptography in recent years. Chaotic maps are often used in encrypting images. Chaos is applied to expand the diffusion and confusion in the image. Due to the desirable properties of nonlinear dynamical systems, such as pseudorandom behaviour, sensitivity to initial conditions, unpredictability and periodicity, chaos-based encryption is suggested as a new and efficient way, to deal with the intractable problem of fast and highly secure image encryption.

4.1.1 Logistic Map for Image Encryption

For image encryption we use logistic map. It will exhibit the chaotic behavior. Both continuous and discrete chaotic maps are available. In this work discrete map is used, this kind of maps usually takes the form of iterated functions. In this work logistic map is used. The logistic map is a simple one dimensional map and is given in Equation (1),

$$x_{n+1} = r x_n (1 - x_n) \quad (1)$$

Logistic map is a polynomial mapping of degree 2. In Equation (1) $X_n \in [0, 1]$ and is known as the phase space of the logistic map, r is the control parameter that controls the behavior of the map.

- With r between 0 to 1 the map is independent of the initial condition.
- For r between 1 to 2 the trajectory will quickly reach the value, map is independent of the initial condition.
- For r between 2 to 3 the trajectory will reach the value in as specific manner that is it will revolve around the value for some time to reach the value.
- With r between 3 to 3.45 for almost all the initial conditions the population will oscillate between two values and these values are depends on the value of b.
- At r approximately 3.57 is the onset of chaos, at the end of the period-doubling cascade. From almost all initial conditions we can no longer see any oscillations of finite period. Slight variations in the initial population yield dramatically different results over time

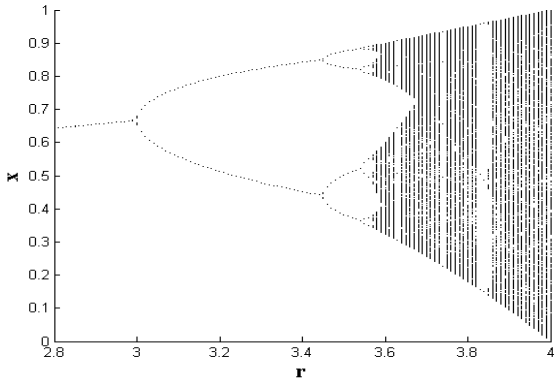

Figure 3.1.1 Bifurcation diagram of logistic map

Beyond r = 4, the values eventually leave the interval [0, 1] and diverge for almost all initial values.

Figure 4.1.1 summarizes the above points and the horizontal axis shows the values of the parameter r while the vertical axis shows the values of x. From Figure 4.1.1 it is clear that for the values above r = 3.82 the map exhibits the chaotic behavior. The map used in this work is a discrete one, it is in the form of iterated function. This map is used because of its easy computation and greater complexity.

4.1.2 Sine Map for Key Encryption

The sine map is same as that of the logistic map chaotic behavior and is defined by Equation (3),

$$x_{n+1} = r \sin(\pi x_n) / 4 \quad (3)$$

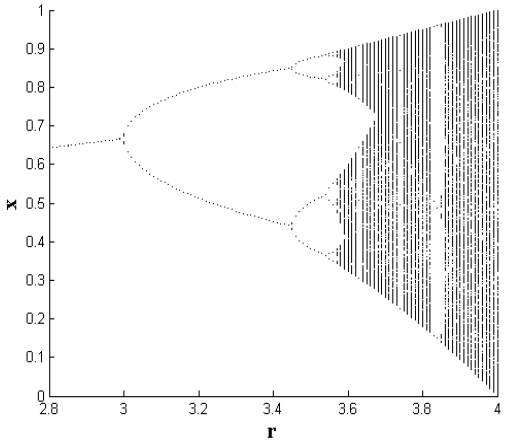

Figure .1.2 Bifurcation diagram of sine map

Where parameter 'r' is in the range of (0 to 4). Figure 4.1.2 shows the chaotic behavior of the sine map it is almost same as that of the logistic map. The sine function provides the good randomness behavior for this chaotic function.

The above mentioned are the chaotic behavior of the map we used for the encryption and decryption process.

5. COPY MOVE FORGERY DETECTION SCHEME

After the completion of Encryption and Decryption process the image is obtained for the process of identification of copy-move forgery. The image is preprocessed before the identification of forgery takes place.

The preprocessing includes:

- Convert the colored image into grayscale image.
- Resize the image into a fixed size of 256 x 256.
- Divide the images into non-overlapping sub blocks.
- Here we divide the image into 64 sub blocks of 32x32 size.

After the preprocessing, we considered some of the following statistical features for the identification of forgery in the images. The features are: Mean, Median, Mode, Variance, Standard Deviation, min, max, kurtosis, skew, Entropy, Moments.

The statistical features are extracted from the images and the features are normalized for better result.

After the normalization of the features, Distance between the blocks had been calculated. The distance measure applied here is Euclidean distance.

The distance between two determines the match. (i.e.) Less distance implies the best match and farthest distance implies the dissimilarities.

While finding the distance, values with zero are eliminated since it defines the distance between same values (i.e.) x-x. A threshold value is fixed for computing the match between the images. The threshold value is the value below which the matches are occurred. Threshold value is fixed based on the trial and error method. Multiple images are taken and check for multiple images and the threshold values are fixed. Finally we have fixed the threshold value by comparing the multiple images and found out the mean of the value as 0.175.

6. WAVELET TRANSFORM

A wavelet is a mathematical function used to divide a given function or continuous time signal into different scale components. Usually one can assign a frequency range to each scale component. Each scale component can then be studied with a resolution that matches its scale. A wavelet transform is the representation of a function by wavelets. The wavelets are scaled and translated copies (known as "daughter wavelets") of a finite length or fast decaying oscillating waveform (known as the "mother wavelet"). Wavelet transforms have advantages over traditional Fourier transforms for representing functions that have discontinuities and sharp peaks, and for accurately deconstructing and reconstructing finite, non-periodic and/or non-stationary signals.

Wavelet transforms are classified into discrete wavelet transforms (DWTs) and continuous wavelet transforms (CWTs). DWTs use a specific subset of scale and translation values or representation grid. Applications of wavelet transform are transform data, and then encode the transformed data, resulting in effective compression and for communication applications.

7. DISCRETE WAVELET TRANSFORM

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time). Applications for discrete wavelet transform are signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression, Practical applications can also be found in signal processing of accelerations for gait analysis, in digital communications.

8. EXPERIMENT RESULT AND DISCUSSIONS

The plain image is encrypted and a key image with changed pixels is taken to calculate the NPCR and UACI. $C_1(i,j)$ is the encrypted plain image and $C_2(i.j)$ is the changed pixel key image.

NPCR and UACI

The number of changing pixel rate **(NPCR)** and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers. The NPCR and UACI are designed to test the number of changing pixels and the number of averaged changed intensity between cipher text images, respectively, when the difference between plaintext images is subtle (usually a single pixel). Although these two tests are compactly defined and are easy to calculate, test scores are difficult to interpret in the sense of whether the performance is good enough. For example, the upper-bound of the NPCR score is 100%, and thus it is believed that the NPCR score of a secure cipher should be very close to this upper-bound.The attacker may have a slight change (modify one pixel) of the plain image to find some meaningful relationships between the plain image and the encrypted. If one minor change in the plain image causes a significant change in the cipher image, this indicates that the encryption scheme resists differential attacks more efficiently. To test the influence of only one pixel change in the plain image over the whole encrypted image, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI),

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UCAI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%$$

Original Image Encrypted Image

NPCR and UACI results =

```
npcr_score: 0.993392944335938
 npcr_pVal: 7.486634401219737e-29
 npcr_dist: [0.996093750000000 5.937181413173676e-08]
uaci_score: 0.228685206992953
 uaci_pVal: 0
 uaci_dist: [0.334635416666667 8.543852862774157e-07]
```

Receiver Operating Characteristics (ROC) Analysis

ROC curves are popularly used as performance metrics for classification task. The ROC curve is acquired by applying a threshold value to the classifier predicted score and obtaining a (TP and FP) value for each threshold to generate the curve.

True positive (TP) = the number of cases correctly identified as Forgery
False positive (FP) = the number of cases incorrectly identified as Forgery
True negative (TN) = the number of cases correctly identified as Mismatch
False negative (FN) = the number of cases incorrectly identified as Mismatch.

Table 8.1 ROC analysis table

	FRAUD	**NO FRAUD**
FRAUD	16	5
NO FRAUD	2	57

Accuracy: The accuracy of a test is its ability to differentiate the forged and not forged cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Senstivity: The sensitivity of a test is its ability to determine the forged cases correctly. To estimate it, we should calculate the proportion of true positive in forged cases. Mathematically, this can be stated as:

$$\text{Sensitivity} = \frac{TP}{TP+FN}$$

Specificity: The specificity of a test is its ability to determine the non forged cases correctly. To estimate it, we should calculate the proportion of true negative in non forged cases. Mathematically, this can be stated as:

$$\text{Specificity} = \frac{TN}{TN+FP}$$

Table 8.2 ROC Result table

Features	**Result Obtained (in %)**
Accuracy	91.25
Specificity	96.61
Sensitivity	76.19
Precision	88.88

9. CONCLUSION AND FUTURE WORK

The detection of forgery in digital images is an interesting topic in forensic science. This paper proposes an effective method for detecting duplicated regions based on the mathematical statistical features in spatial domain. Experiment results demonstrate that the proposed algorithm is able to detect and precisely locate multiple instances of copy–move forgery in a single image. Next our aim is to detect the copy move forgery in wavelet domain using DWT. Also for precise identification of forgery we are planned to use overlapping sub blocks concept.

10. REFERENCE

[1] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A SIFT-based forensic method for copy–move attack detection and transformation recovery, IEEE
Trans. Inform. Forensics Sec. 6 (2011) 1099–1110.
[2] O.M. Al-Qershi, B.E. Khoo, Passive detection of copy–move forgery in digital images: states-of-the-art, Forensic Sci. Int. 206 (1) (2013) 284–295.
[3] S. Bayram, H.T. Husrev, N. Memon, An efficient and robust method for detecting copy–move forgery, in: Proceedings of the IEEE International
Conference on Acoustics, Speech and Signal Processing, 2009, pp. 1053–1056.
[4] A. Costanzo, I. Amerini, R. Caldelli, M. Barni, Forensic analysis of SIFT keypoint removal and injection, IEEE Trans. Inform. Forensics Sec. 9 (9) (2014)
1450–1464.
[5] L. Chen, W. Lu, J. Ni, W. Sun, J. Huang, Region duplication detection based on Harris corner points and step sector statistics, J. Vis. Commun. Image Rep.
24 (2013) 244–254.
[6] CoMoFoD Database. <http://www.vcl.fer.hr/comofod>.
[7] N. Dalal, B. Triggs, Histograms of oriented gradients for human detection, Comput. Vis. Pattern Recognit. (2005) 20–25.
[8] J. Fridrich, D. Soukal, J. Lukas, Detection of copy–move forgery in digital images, in: Proceedings of Digital Forensic Research Workshop, 2003, pp. 19–
23.
[9] J. Fridrich, Methods for tamper detection in digital images, in: Proceedings of the ACM Workshop on Multimedia and Security, 1999, pp. 19–23.
[10] T. Gloe, M. Kirchner, A. Winkler, R. Behme, Can we trust digital image forensics? in: Proceedings of the 15th International Conference on Multimedia,
2007, pp. 78–86.
[11] S. Khan, A. Kulkarni, An efficient method for detection of copy–move forgery using discrete wavelet transform, Int. J. Comput. Sci. Eng. 2 (2010) 1801–
1806.
[12] X. Kang, S. Wei, Identifying tampered regions using singular value decomposition in digital image forensics, in: Proceedings of International
Conference on Computer Science and Software Engineering, 2008, pp. 926–930.
[13] B. Mahdian, S. Saic, Detection of copy–move forgery using a method based on blur moment invariants, Forensic Sci. Int. 171 (2007) 180–189.
[14] D. Lowe, Object recognition from local scale-invariant features, Proc. Int. Conf. Comput. Vis. 2 (1999) 1150–1157.