I J C T A, 9(7), 2016, pp. 3205-3209 ISSN: 0974-5572

Cyber Forensic Security Using Fingerprint Digital Image by Comparison Over Manuscripts and Archives Digital Images Database and Dyadic Scale Space Extrema Identification

Gouri M.S.* and R.V. Sivabalan**

ABSTRACT

Forensic accuracy on digital fingerprint images poses critical challenge for the digital forensic analysis. There are many fingerprint matching systems available Also, content-based fingerprint matching does not provide robustness against content change attacks. In this paper, we propose a three-step digital fingerprint image method called, Enhanced Dyadic Scale Space Extrema Identification (EDSSEI). The Forensic Digital Image Content Hashing technique is integrated with EDSSEI method to authenticate the multimedia information without any content change attacks. The assessment rule based linear hashing in EDSSEI method overcomes the global fingerprints attacks. The effectiveness of our method is demonstrated by a thorough evaluation and comparison over Manuscripts and Archives Digital Images Database (MADID). The performance improvement thus achieved makes Enhanced Dyadic Scale Space Extrema Identification superior to other state-of-the-art woks

Keywords: *Digital forensic analysis, Fingerprint matching, Dyadic Scale-space*

1. INTRODUCTION

The information technological persons across the earth are spending enormous time and cost for securing the information using security related mechanisms. So to overcome the cybercrime activities during digital data transfer through proper communication channel is to perform the forensics analysis.. Copy Detection using Content-based Fingerprinting (CD-CF) [1] used approximate search algorithms to yield high true positive and minimize the false positive rate. Anti-forensic techniques [2] using image transform coefficient reduced the rate of image tampering. The issues related to security are addressed in EDSSEI method by applying Dyadic Scale Space model. **A** social network integrates organizations through one or more specific types of interdependency, wherein a group of users share multimedia contents, as well as other resources. In [3], game theory strategy was applied for multimedia fingerprinting using bargaining behaviour as non-cooperative model. Using EDSSEI method, Forensic Digital Image Content Hashing is applied. In [4], fingerprint quality evaluation for mobile users was performed in an extensive manner using Automatic Fingerprint Authentication System (AFAS) performed.

Based on the aforementioned methods and techniques, in this paper, Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) is presented. The novelty and advantages of the proposed method include a Dyadic Scale Space model is proposed to fragment fingerprint digital image for reducing noise and improving security aiming at improving the crime detection rate using different numbers of samples. This paper is structured as follows. Section 2 presents an overview with the help of block diagram and algorithm.

* Research Scholar, CSE Department, Noorul Islam University, *Email: gourimohans@gmail.com*

** Associate Professor, MCA Department, Noorul Islam University, *Email: rvsivan@gmail.com*

Section 3 gives an idea of the experiments settings with the help of parametric definitions. Section 4 describes in detail using table and graph form, and Section 5 draws a conclusion.

2. ENHANCED DYADIC SCALE SPACE EXTREMA IDENTIFICATION

In this advanced era, digital multimedia data plays a vital role for fast and efficient communication. In this section, we briefly explain the Enhanced Dyadic Scale Space Extrema Identification method.

2.1. Dyadic Scale Space

This section introduces the Dyadic Scale Space model to enhance the fingerprint digital image. Dyadic Scale Space is a linear space system with the objective to reduce noise.

As shown in the block diagram below, Dyadic Scale Space model initially based on Gaussian scale extracts different set of scale space by fragmenting fingerprint digital image. The ridges are alternated with valleys and a flow-like pattern fingerprint in digital image is comprised. Initially the fingerprint digital image is fragmented into a progression of images and the noise is reduced which is present in different scales. The second step includes combining of images to obtain more reliable fingerprint digital image. During each step, the noise present in the fingerprint digital image is considerably minimized. Once different steps or division are performed, the final improvised fingerprint digital image is obtained. The EDSSEI method extracts the fingerprint digital image that was decomposed through Gaussian Dyadic Scale model into a more compact representation called, Forensic Digital Image Content Hashing. For efficient comparison of training and testing fingerprint digital images pre-processing operations like scaling and rotation are used.

2.2. Forensic Digital Image Content Hashing

The second step in the design of EDSSEI method is the integration of Forensic Digital Image Content Hashing technique with EDSSEI method. This is mainly done to authenticate the multimedia information

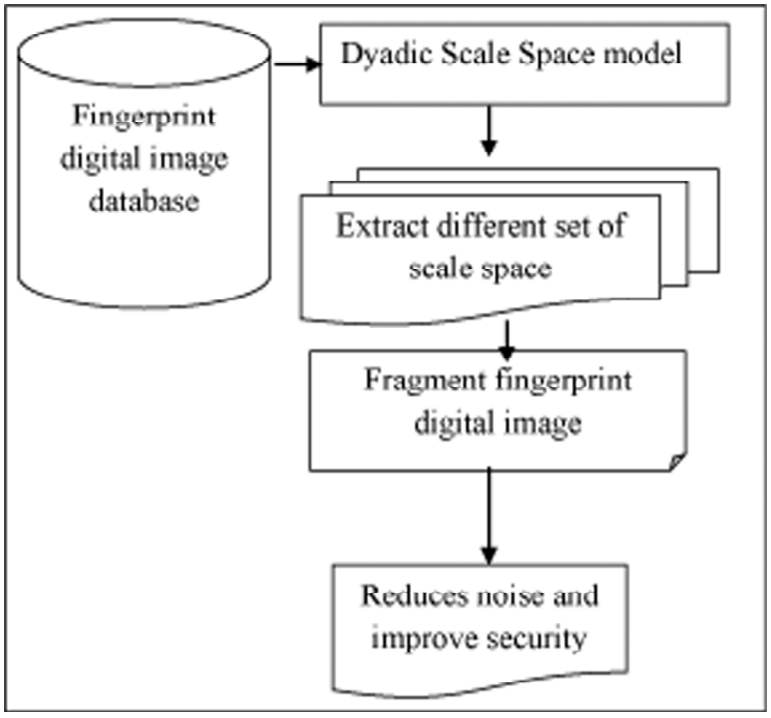

Figure 1: Block diagram of Dyadic Scale Space model

without any content change attacks. This efficiently evaluate the parameters of geometric transforms and helps in detecting the occurrence of any content change attacks.

2.3. Binary assessment rule

The final step in the design of EDSSEI method is the application of binary assessment rule. This is done by taking the successive value of the training and test digital images and thus by applying Binary assessment rule, the global fingerprint attacks are minimized in an efficient manner. Hashing technique is used to provide forensics security on fingerprint digital images.The rotated and scaled image are compared to the original fingerprint digital image. Forensics security on fingerprint digital images is provided through the hashing technique with discriminate capability.The testing and training fingerprint digital images are properly aligned based on the gradient magnitude image.

3. DISCUSSION

The Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method is compared against the existing Fingerprint Matching using GPU (FM-GPU) [5] and Copy Detection using Content-based Fingerprinting (CD-CF) [2] method. The experimental results using MATLAB are compared and analysed with the aid of graph form given below.

3.1. Scenario 1: Security level on transferring digital data

The convergence plot for 35 images is depicted in figure 2 and table 1. From the figure we can note that the proposed EDSSEI method achieved maximum security level on transferring digital data when compared to other methods.

Table 1
Tabulation for security level on transferring digital data

No of images	*Security levelmon transferring digital data (ips)*		
	Edssei	*FM-GPU*	*CD-CF*
5	4	3	2
10	8	7	5
15	13	11	9
20	17	15	12
25	22	19	17

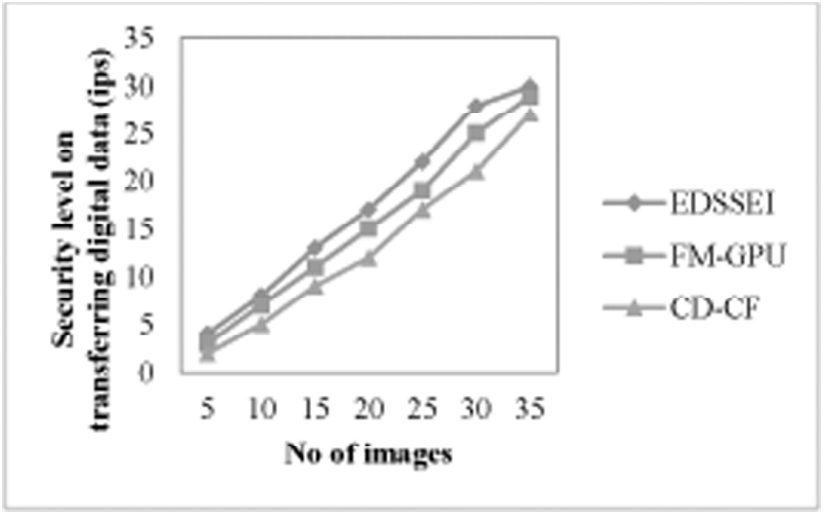

Figure 2 Measure of security level on transferring digital data

The figure shows that when the number of images increases the security level on transferring digital data increases and shows that a drift decrease occurs when 35 images were used. The security level on transferring digital data is increased with the application of Dyadic Scale Space model. The Dyadic Scale Space model in EDSSEI method effectively constructs progression of images in a parallel manner for the test and training sample images for multiple scales and therefore the security level on transferring digital data is improved by 13.19% compared to FM-GPU [5]. Moreover, by applying Gaussian Dyadic Scale Algorithm, significant noise reduction is made using Gaussian and Dyadic model. As a result, the security level on transferring digital data is increased by 29.34% compared to CD-CF [1].

3.2. Scenario 2: Recognition accuracy

Table 2 shows the recognition accuracy efficiency over 35 different images provided as input using MATLAB. From the figure, with an increase in the number of images provided, the recognition accuracy efficiency also increases, though the curve observed is not linear. However, the recognition accuracy efficiency in an increasing stage till 15 images was considered. But with an increase in the number of images with 10, the recognition accuracy efficiency decreased and then increased with 25 images. This is because of the different images gathered consists of a combination of digital images that includes postures, drawing text documents and so on. As these images are not similar, the changes in the recognition accuracy are also being observed. As a result, the percentage increase or decrease in recognition accuracy efficiency does not remain the same.

Table 2
Tabulation for recognition accuracy

No of images	*Recognition accuracy (%)*		
	Edssei	*FM-GPU*	*CD-CF*
5	78.35	61.46	38.95
10	81.49	70.49	62.47
15	83.55	72.55	64.53
20	80.25	69.25	61.23
25	84.19	73.19	65.17
30	82.13	71.13	63.11

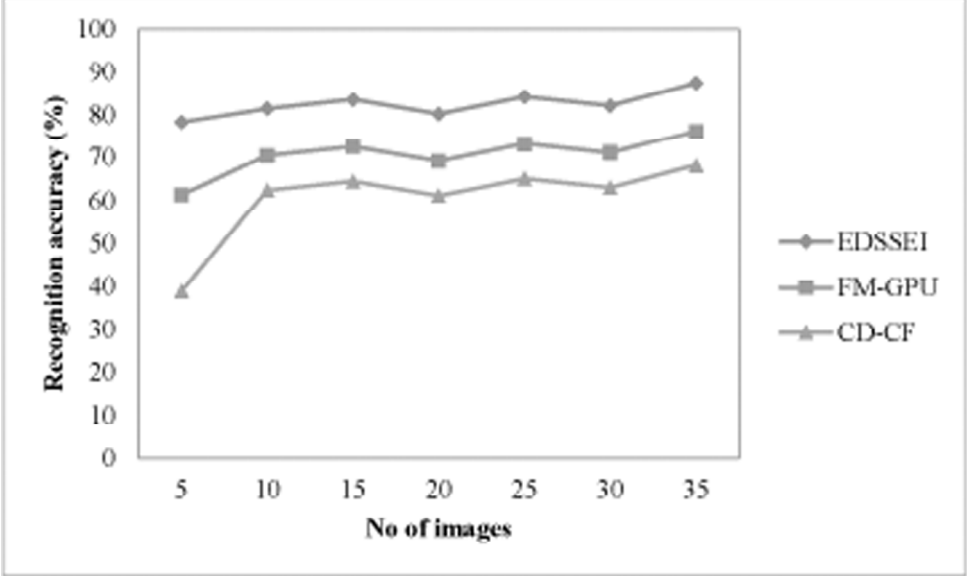

Figure 3: Measure of recognition accuracy

4. CONCLUSION

Different features like temporal, spatial colour-space-based even though provide high copyright protection and security for the conventional forensic security on multimedia based digital data may not give satisfactory result for content change attack. Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method has been implemented to increase the security level during the transfer of digital data and content of finger print images. This is a three step model. First step involves deriving different set of scale space using Dyadic Scale Space, the second step includes authentication of multimedia information using Forensic Digital Image Content Hashing technique and the final step is performing of binary assessment rule with authenticated multimedia information introduced in EDSEEI. Comparison of the performance is done with many different system parameters, and evaluated the performance in terms of different metrics, such as recognition accuracy and security level on transferring digital data with respect to different number and size of images.

REFERENCES

[1] Mani Malek Esmaeili., Mehrdad Fatourechi., and Rabab Kreidieh Ward., "A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 6, No. 1, March 2011.

[2] Matthew C.Stamm, and K. J. Ray Liu, "Anti-Forensics of Digital Image Compression", IEEE Transactions on Information Forensics and Security, Volume 6,Issue 3, September 2011, pp. 1050-1065.

[3] W. Sabrina Lin, H. Vicky Zhao, and K. J. Ray Liu, "Game-Theoretic Strategies and Equilibriums in Multimedia Fingerprinting Social Networks", IEEE Transactions on Multimedia, Volume 13, Issue 2, April 2011, pp. 191-205.

[4] Giuseppe Vitello, Vincenzo Conti, Salvatore Vitabile, and Filippo Sorbello, "Fingerprint Quality Evaluation in a Novel Embedded Authentication System for Mobile Users", Hindawi Publishing Corporation, Mobile Information Systems, Volume 2015, September 2014, pp. 1-14.

[5] Shakeel Ahmad, Raouf Hamzaoui, and Marwan M. Al-Akaidi, "Unequal Error Protection Using Fountain Codes With Applications to Video Communication", IEEE Transactions on Multimedia, Volume 13, Issue 1, February 2011, pp. 92-101.

[6] Hassan Mansour, Panos Nasiopoulos, and Vikram Krishnamurthy, "Rate and Distortion Modeling of CGS Coded Scalable Video Content", IEEE Transactions on Multimedia, Volume 13, Issue 2, April 2011, pp. 165-180.