IJCTA, 9(36), 2016, pp. 201-211

Dyadic Scale Space Extrema Identification for Cyber Forensic Security Using Fingerprint Digital Image

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. Minutiae matching remain one of the oldest and most popular fingerprint matching models. On one hand implementation of minutiae matching is simple, and, on the other hand, this does not achieve higher forensic accuracy rate. 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 proposed method consists of three main steps. (1) derives different set of scale-space fingerprint digital image pixels; (2) authentication of multimedia information; and (3) perform binary assessment rule with authenticated multimedia information. The Dyadic Scale Space in EDSSEI derives different set of scale-space fingerprint digital image pixels for analyzing the characteristics and spatial inconsistencies. 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. Experiment is conducted on factors such as recognition accuracy, security level on transferring digital data, crime data detection rate, performance speed up. Experiment results show that the proposed method achieves better performance in improving the recognition accuracy by 20.61% and improves the improving the security level on transferring digital data by 21.26% compared to the state-of-the-art works.

Keywords : Minutiae matching, Digital forensic analysis, Fingerprint matching, Dyadic Scale-space, Binary assessment rule.

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 cyber crime activities during digital data transfer through proper communication channel is to perform the forensics analysis. Many works has been focused on securing the fingerprint digital images using various mechanisms. Fingerprint Matching using Graphics Processing Units (FM-GPU) [1], applied Minutia Cylinder Code (MCC) to enhance fingerprint matching mechanism. Copy Detection using Content-based Fingerprinting (CD-CF) [2] used approximate search algorithms to yield high true positive and minimize the false positive rate.

Anti-forensic techniques [3] using image transform coefficient reduced the rate of image tampering. Optimal fusion algorithms [4] using Maximum Log-likelihood Ratio-based (MLR) scheme resulted in

* Research Scholar, Department of Computer Science and Engineering, Noorul Islam University, Kanyakumari District

the improvement of accuracy of images being detected. Forward Error Correction (FEC) [5] applied to Scalable Video Coding (SVC) resulted in the improvement of efficiency in transmission with high video quality. In [6], Mean Absolute Difference (MAD) was evaluated to arrive at the accuracy of scalable video content. Though the methods presented above improved the rate of accuracy, but the security aspects remained unaddressed. 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 [7], game theory strategy was applied for multimedia fingerprinting using bargaining behavior as non cooperative model. Visual patterns and textual concepts were applied in [8] to improve the alignment performance using sentence-based alignment. In [9], optimal bandwidth assignment was achieved using Multiple Description Coding (MDC) resulting in the improvement for maximal user satisfaction. An adaptive mulsemedia framework was designed in [10] with the objective of delivering scalable video using fine grained adaptation modules.

In [11], an empirical model was presented aiming at improving the mean efficiency using object-related phenomena. Efficient heuristic methods was applied in [13] called, Domain Adaptive Linear Combination aiming at improving the Mean Inferred Average Precision (MIAP). The image-based kernel fingerprinting in [14] using approximate matching tool resulted in the improvement of content similarity and efficiency. Though efficiency was the key in the above mentioned papers, the content change attack during multimedia transmission remained unsolved. Using EDSSEI method, Forensic Digital Image Content Hashing is applied.

A fingerprint encryption scheme based on irreversible function using irreversible transforming function was presented in [15]. This resulted in the improvement of security by determining only the fingerprint features. In [16], fingerprint quality evaluation for mobile users was performed in an extensive manner using Automatic Fingerprint Authentication System (AFAS). Latent Fingerprint Matching using Total Variation (TV) decomposition model was performed in [17] resulting in the improvement of robustness and accuracy. In [18], a survey of fingerprint matching model was performed. Partial Encryption and Discrete Wavelet Transform [19] was applied to improve the flexibility of fingerprint efficiency model. Digital Watermarking and Fingerprinting techniques was applied in [20] with the objective of reducing the attack.

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: 1) a Dyadic Scale Space model is proposed to fragment fingerprint digital image for reducing noise and improving security; 2) the Forensic Digital Image Content Hashing technique is proposed to take advantage of minimizing content change attack; and 3) the Binary assessment rule of the proposed algorithm is able to deal with the training samples aiming at improving the crime detection rate using different numbers of samples. Experiments on Manuscripts and Archives Digital Images Database (MADID) show the effectiveness of the proposed algorithm.

This paper is structured as follows. Section 2 presents an overview of the Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method with the aid of block diagram and algorithm. Section 3 describes the experiments settings with the parametric definitions. Section 4 discusses in detailed 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. Some of the real world applications of digital data include financial documents, medical records, journalism and so on. 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 by minimizing the noise and therefore improving the security level on transferring digital data. Dyadic Scale Space is a linear space system that derives different set of scale-space fingerprint digital image pixels. The objective of using Dyadic Scale Space model is that with the increase of the scale, noise is significantly reduced in a gradual manner. Figure 1 shows the block diagram of Dyadic Scale Space model.

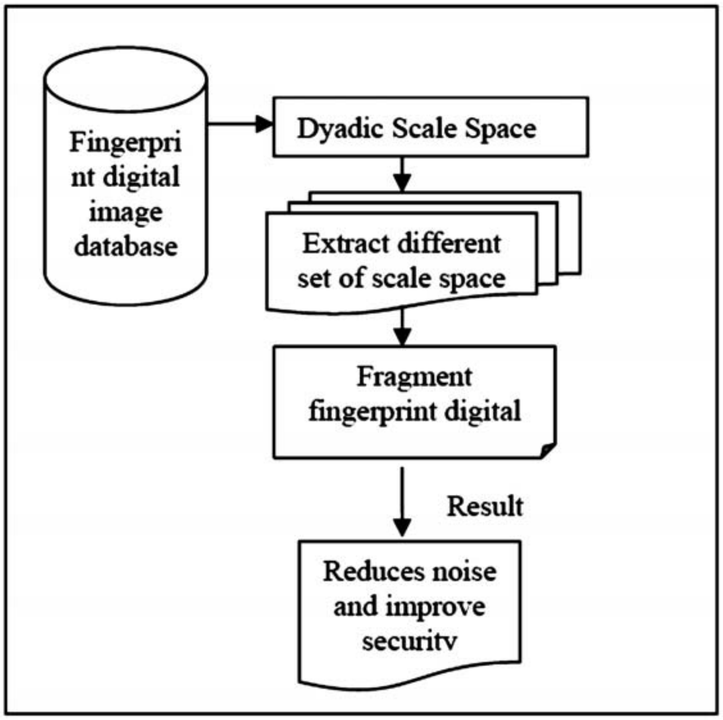
Fingerprint digital image database
Dyadic Scale Space
Extract different set of scale space
Fragment fingerprint digital
Result
Reduces noise and improve securitv

Figure 1: Block diagram of Dyadic Scale Space model

As shown in the block diagram, Dyadic Scale Space model initially extracts different set of scale space by fragmenting fingerprint digital image based on Gaussian scale. The fingerprint in digital image comprises of a flow-like pattern where the ridges are alternated with valleys. The proposed EDSSEI method initially fragments the fingerprint digital image into a progression of images with the objective of reducing the noise present in different scales. Next, the images are combined to obtain more reliable fingerprint digital image. During each iteration's, the noise present in the fingerprint digital image is considerably minimized. Once different iterations are performed, the final improvised fingerprint digital image is obtained.

The fingerprint digital image is decomposed into series of different scales for analyzing the characteristics and spatial inconsistencies. The proposed EDSSEI method uses Dyadic Scale for efficient decomposing of fingerprint digital image and is mathematically formulated as given below.

$$\delta_j = 2^j,$$

where $$j = 1,2,3,\ldots..,n \tag{1}$$

From (1), the scale 'δ' in the above representation is referred to as the dyadic, whereas the scale space form is referred to as the Dyadic Scale Space. Let us consider a fingerprint digital image '$\text{Image}_i = \text{Image}_1$, $\text{Image}_2,\ldots,\text{Image}_n$', at multiple scales is formulated as given below.

$$G_s = \text{Image}\,(i, j, \theta) \tag{2}$$

From (2), the Guassian scale 'G_s' for an image 'Image' with pixel values 'i' and 'j' at 'θ' hashing detects the feature in fingerprint digital image aiming at reducing the noise. By applying Dyadic Scale Space, the enhanced fingerprint digital image is formulated as given below.

$$E_{\text{Image}} = \text{Image} * G2^{j} (i, j, \theta) \tag{3}$$

With the enhanced image obtained from (3), the noise present in the fingerprint digital image is minimized in a significant manner. This in turn improves the security level on transferring digital data. Figure 2 shows the algorithmic description of Gaussian Dyadic Scale Algorithm.

```
Input : Fingerprint digital image ‘$Image_i = Image_1, Image_2, \ldots, Image_n$’,
Output : Secured Fingerprint digital image representation
Step 1: Begin
Step 2: For each Fingerprint digital image $Image^i$
Step 3: Evaluate dyadic scale using (1)
Step 4:  Evaluate multiple scales with the aid of Guassian model using (2)
Step 5: Extract the enhanced image by applying Gaussian and Dyadic model using (3)
Step 6 : End for
Step 7: End
```

Figure 2: Gaussian Dyadic Scale Algorithm

As shown in the figure, with the objective of reducing the noise present in the image and therefore increasing the security while transferring fingerprint digital data, Gaussian and Dyadic Scale is applied. For each fingerprint digital image, dyadic scale is evaluated. With the objective of reducing the noise, for forming visual model at multiple representations multiple scales are formed. Followed by while, the enhanced image is extracted aiming at improving the security during digital data transfer.

2.2. Forensic Digital Image Content Hashing

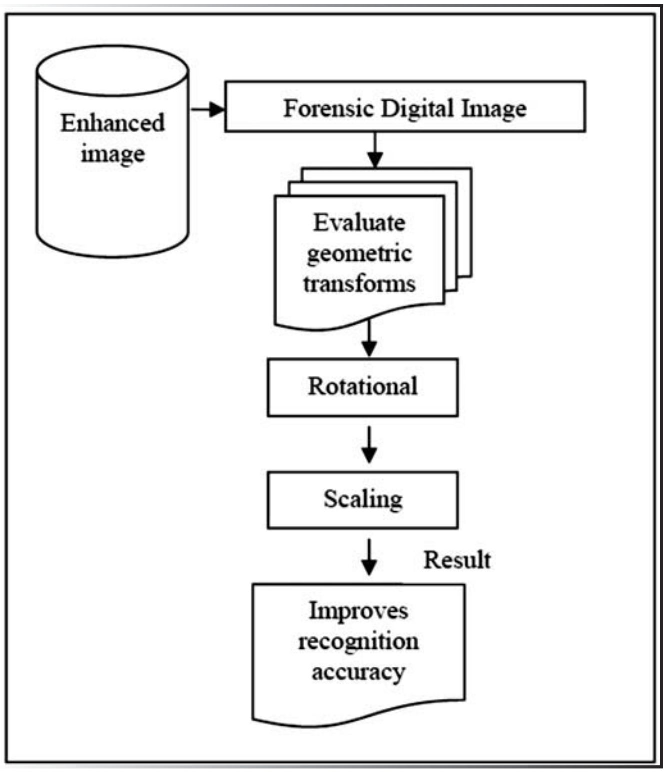

Figure 3: Block diagram of Forensic Digital Image Content Hashing

Type equation here.

The second step in the design of EDSSEI method is the integration of Forensic Digital Image Content Hashing technique with EDSSEI method to authenticate the multimedia information without any content change attacks. The objective of applying Forensic Digital Image Content Hashing in EDSSEI method is to efficiently evaluate the parameters of geometric transforms and detect the occurrence of any content change attacks. Figure 3 shows the Block diagram of Forensic Digital Image Content Hashing.

As shown in the figure, the Block diagram of Forensic Digital Image Content Hashing evaluates geometric transforms. The resultant obtained image by applying the rotation and scaling transform improves the recognition accuracy.

The EDSSEI method extracts the decomposed fingerprint digital image obtained as a result of Gaussian Dyadic Scale model into a more compact representation called, Forensic Digital Image Content Hashing. Symmetrical hashings like rotation, scaling are the most predominant pre-processing operations for efficient comparison of training and testing fingerprint digital images. In this section, Forensic Digital Image Content Hashing for efficient evaluation of rotation and scaling is performed in an efficient manner.

In order to extract the hashing of fingerprint digital images, the direction of image plays the pivotal role. Let us consider the enhanced image ‘$\mathrm{E}_{\mathrm{Image}}$ (i, j)’ after removal of noise using Gaussian and Dyadic Scale, the EDSSEI initially applies the gradient based edge detector. It is formulated as given below.

$$\mathrm{GradE}_{\mathrm{Image}}(i, j) = i'\left(\frac{\partial \mathrm{E}_{\mathrm{Image}}(i,\ j)}{\partial \mathrm{E}_{\mathrm{Image}}}\right) + j'\left(\frac{\partial \mathrm{E}_{\mathrm{Image}}(i,\ j)}{\partial \mathrm{E}_{\mathrm{Image}}}\right) \tag{4}$$

From (4), ‘$\left(\frac{\partial \mathrm{E}_{\mathrm{Image}}(i,\ j)}{\partial \mathrm{E}_{\mathrm{Image}}}\right)$’ represents the gradient in the ‘i^{th}’ direction ‘$\left(\frac{\partial \mathrm{E}_{\mathrm{Image}}(i,\ j)}{\partial \mathrm{E}_{\mathrm{Image}}}\right)$’ represents the gradient in the ‘j^{th}’ direction. In order to obtain the edge, the gradient magnitude is evaluated and formulated as given below.

$$\mathrm{Grad}_m\mathrm{E}_{\mathrm{Image}} = \sqrt{\mathrm{GradE}_{\mathrm{image}}(i^2) + \mathrm{GradE}_{\mathrm{image}}(j^2)} \tag{5}$$

From (5), the gradient magnitude is obtained the Forensic Digital Image Content rotate aiming at improving the recognition accuracy is formulated as given below.

$$\mathrm{Rotation}_{\mathrm{Image}}\ (m\ ,\theta) = \int_1^n \mathrm{Grad}_m\mathrm{E}_{\mathrm{Image}}(m \cos \theta\ ) + \mathrm{Grad}_m\mathrm{E}_{\mathrm{Image}}\ (m \sin \theta\ ) \tag{6}$$

Followed by rotation, the Forensic Digital Image Content scaling (i.e. the scaled image) is formulated as given below.

$$\mathrm{Scaled}_{\mathrm{Image}} = (s)^*\ f\,'\ (\mathrm{Rotation}\ (m\ ,\theta)) \tag{7}$$

From (7), the scaled image ‘’ is obtained by applying a scaling factor ‘’ to the resultant rotated fingerprint digital image. This in turn efficiently detects the occurrence of any content change attacks and improves the recognition accuracy in the receiving end during multimedia digital data transfer. Figure 4 shows the algorithmic description of Digital Image Hashing.

```
Input : Enhanced image ‘$E_{Image}$’
Output : Authenticated multimedia information with reduced content change attack
Step 1: Begin
Step 2: For each enhanced image ‘$E_{Image}$’
Step 3: Perform gradient based edge detector using (4)
Step 4: Obtain gradient magnitude using (5)
Step 5: Perform rotational transform with the gradient magnitude image using (6)
Step 6: Perform scaling transform with the gradient magnitude image using (7)
Step 7: End for
Step 8: End
```

Figure 4: Forensic Digital Image Hashing algorithm

As shown in the figure, the Forensic Digital Image Hashing algorithm consists of four steps. For each enhanced image obtained by applying Gaussian and Dyadic Space, gradient based edge detector is performed to obtain the edge. Followed by this, the gradient magnitude is applied to obtain the edge and therefore improve the fingerprint digital recognition accuracy. Finally, the rotational and scaling transform is applied to the gradient magnitude image aiming at reducing the content change attack.

2.3. Binary assessment rule

The final step in the design of EDSSEI method is the application of binary assessment rule. The Binary assessment rule takes the successive value of the training and test digital images. By applying Binary assessment rule, based on the linear hashing, the global fingerprint attacks are minimized in a significant manner. Forensics security on fingerprint digital images is provided through the hashing technique with discriminate capability.

The binary assessment rule in EDSSEI method global fingerprint attacks by comparing the original fingerprint digital image to the rotated and scaled image. Forensics security on fingerprint digital images is provided through the hashing technique with discriminate capability. For this binary assessment rule to perform well, the testing and training fingerprint digital images are properly aligned based on the gradient magnitude image. It is mathematically formulated as given below.

If $\text{Image}_i = \text{Rotation}_{\text{Image}}\ (m, \theta)$ and

If $\text{Image}_i = \text{Scaled}_{\text{Image}}$ then "No fingerprint attacks"

If $\text{Image}_i <> \text{Rotation}_{\text{Image}}\ (m, \theta)$ and

If $\text{Image}_i <> \text{Scaled}_{\text{Image}}$ then "Presence of fingerprint attacks"

Based on the above two conditions, the presence of fingerprint attacks are detected in an efficient manner, improving the crime detection rate.

3. EXPERIMENTAL SETTINGS

Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method uses MATLAB coding to authenticate the multimedia information. This method is widely used to perform efficient authentication of fingerprint digital image with the tests and training samples. Manuscripts and Archives Digital Images Database (MADID) are taken to perform the experimental work. The training model for MADID database consists of digital reproductions of photographs, posters, drawings, text documents, and other images taken from the research collections of Manuscripts and Archives, Yale University Library.

The performance of Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method is compared to that of the Fingerprint Matching using GPU (FM-GPU) [1], a method for performing efficient fingerprint matching and Copy Detection using Content-based Fingerprinting (CD-CF) [2], a fast video copy detection system. The tests on MADID were conducted to evaluate four parameters: security level on transferring digital data, recognition accuracy, content change attack and crime detection rate.

The security level on transferring digital data measures the rate at which the security is attained. The security level is mathematically formulated as given below.

$$S = (\text{Images}_s - \text{Images}_d) \tag{8}$$

From (8), 'S' refers to the security level whereas the 'Images_s' refers to the images being sent and 'Images_d' the images being dropped respectively. Higher the security level on transferring data, more efficient the method is said to be. The recognition accuracy measures the rate at which the images are received at the receiving end. It is measured in terms of percentage (%). The recognition accuracy is mathematically formulated as given below.

$$A = \left(\frac{\text{Images}_r}{\text{Images}_s}\right) * 100 \tag{9}$$

From (9), 'A' refers to the recognition accuracy whereas the 'Images$_r$' refers to the images being received and 'Images$_s$' the images sent respectively. Higher the recognition accuracy on transferring data, more efficient the method is said to be. The rate of content change attack measures the change in content while transferring fingerprint digital images. The content change attack is the difference between the actual image size and the modified image size. It is mathematically formulated as given below.

$$CCA = \text{Image Size-Modified Image Size} \qquad (10)$$

From (10), the content change attack '' is measured. Lower the content change attack, more efficient the method is said to be.

4. DISCUSSION

The Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method is compared against the existing Fingerprint Matching using GPU (FM-GPU) [1] and Copy Detection using Content-based Fingerprinting (CD-CF) [2] method. The experimental results using MATLAB are compared and analyzed with the aid of graph form given below.

4.1. Scenario 1: Security level on transferring digital data

The convergence plot for 35 images is depicted in figure 5 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 level on 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
30	28	25	21
35	30	29	27

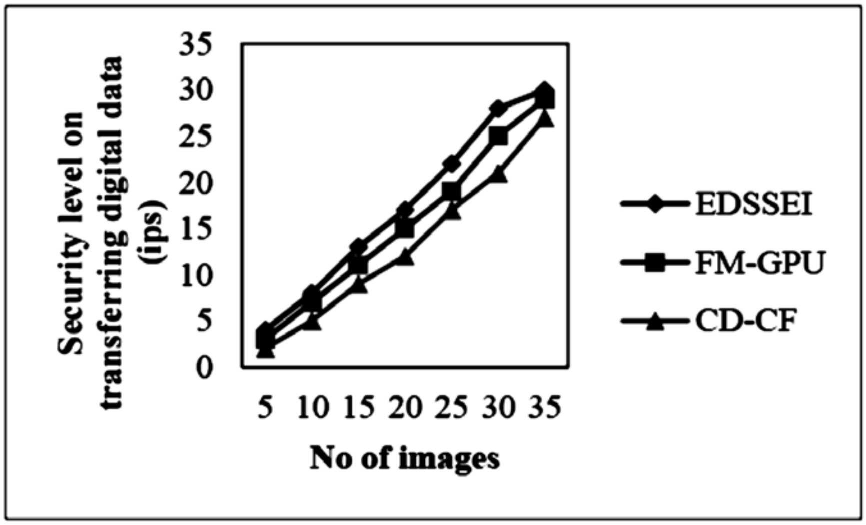

Figure 5: Measure of security level on transferring digital data

The figure shows that the security level on transferring digital data increases with the increase in the number of images 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 [1]. 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 [2].

4.2. 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
35	87.22	76.22	68.20

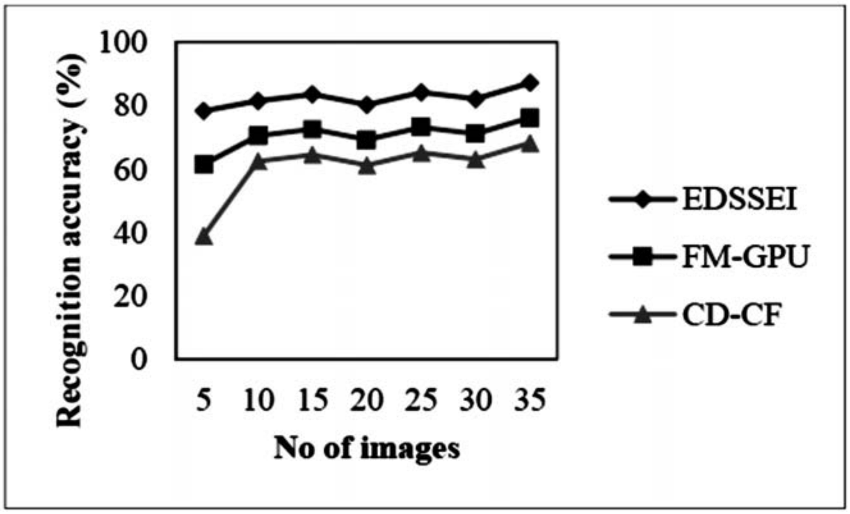

Figure 6: Measure of recognition accuracy

Comparatively from figure 6, the recognition accuracy efficiency is improved using the proposed method EDSSEI. The Recognition accuracy rate in EDSSEI method is improved with the application of Forensic Digital Image Content Hashing technique that uses different orientations (i.e. rotation and scaling) for training and testing fingerprint digital images. This in turn results in higher recognition accuracy rate by 14.42% compared to FM-GPU [1] on working with the test and training sample images. In addition using EDSSEI method by applying the Gaussian and Dyadic Scale with the aid of gradient based edge detector results in the improvement of recognition accuracy by 26.80% compared to CD-CF [2].

4.3 Scenario 3: Content change attack.

Convergence characteristics for the measure of content change attack rate for 35 test images with varying digital reproduction of photographs, drawings, text documents and other images taken from the research are considered and compared with two other methods and are shown in table 3.

Table 3

Tabulation for content change attack

Image size (KB)	*Content change attack (KB)*		
	EDSSEI	*FM-GPU*	*CD-CF*
100	9	13	15
200	15	23	26
300	22	30	33
400	31	39	42
500	43	51	54
600	54	63	66
700	68	76	79

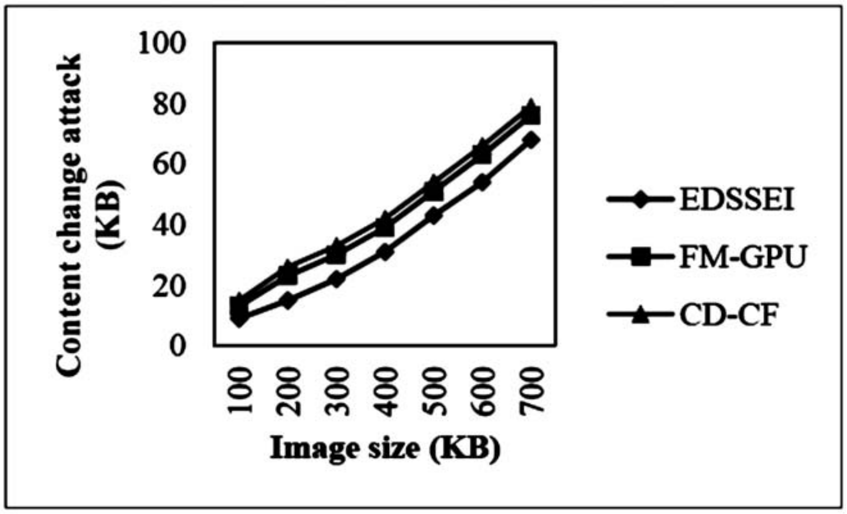

Figure 7: Measure of content change attack

The targeting results of content change attack rate on performing digital data transfer using EDSEEI method is compared with two state-of-the-art methods [1], [2] in figure 7 is presented for visual comparison based on the size of images. Our method differs from the FM-GPU [1] and CD-CF [2] in that we have incorporated Forensic Digital Image Content Hashing technique. The Forensic Digital Image Content Hashing technique designs the orientation model using rotation and scaling in an efficient manner for performing digital data transfer. As a result, the content change attack while transferring digital data using ELSEEI method is reduced by 29.56% compared to FM-GPU. Furthermore, by obtaining gradient magnitude further reduces the content change attack during digital data transfer by 41.35% compared to CD-CF.

4.4. Scenario 4: Crime detection rate

Table 4 shows the crime detection rate using the three methods, EDSEEI, FM-GPU [1] and CD-CF [2] respectively. The crime detection rate in table 4 was measured with the aid of 35 images extracted from the Manuscripts and Archives Digital Images Databases.

Table 4
Tabulation for crime detection rate

Methods	*Crime detection rate (%)*
EDSSEI	83.14
FM-GPU	75.32
CD-CF	68.19

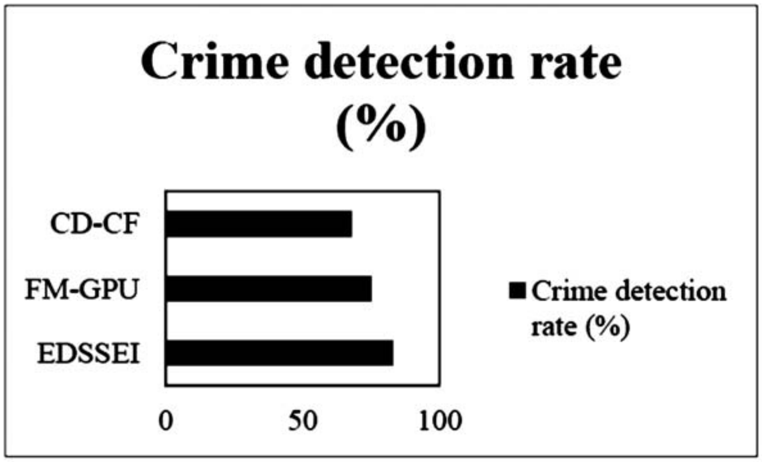

Figure 8: Measure of crime detection rate

Figure 8 shows the measure of crime detection rate with respect to 35 different images obtained from MADID. The crime detection rate using EDSEEI method is improved when compared to two other methods [1] and [2]. This is due to the application of binary assessment rule. By applying binary assessment rule, the test and training images are considered and further compared with the oriented images (i.e. images obtained from rotation and scaling). This in turn improves the crime detection rate using EDSEEI method by 9.40% compared to FM-GPU and 9.46% compared to CD-CF respectively.

5. CONCLUSION

The conventional forensic security on multimedia based digital data designed for high performance fingerprint matching system based on differing features like temporal, spatial color-space-based though provide high copyright protection and security may not give satisfactory result for content change attack. To improve the security level on transferring digital data and content change attack on fingerprint digital images, Enhanced Dyadic Scale Space Extrema Identification (EDSSEI) method has been implemented. The three step model, deriving different set of scale space using Dyadic Scale Space, authenticating multimedia information using Forensic Digital Image Content Hashing technique and perform binary assessment rule with authenticated multimedia information introduced in EDSEEI method resulted in the significant improvement over the state-of-the-art methods. We compared the performance with many different system parameters, and evaluated the performance in terms of different metrics, such as recognition accuracy, security level on transferring digital data, content change attack, crime detection rate with respect to different number and size of images. The results show that EDSEEI method offers better performance with an improvement of crime detection rate by 9.43% and minimize the content change attack by 35.46% compared to FM-GPU and CD-CF respectively.

6. REFERENCES

1. Pablo David Gutiérrez., Miguel Lastra., Francisco Herrera., and José Manuel Benítez., "High Performance Fingerprint Matching System for Large Databases Based on GPU," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014
2. 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
3. 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,Pages 1050-1065.
4. Takao Murakami, Kenta Takahashi, and Kanta Matsuura, "Toward Optimal Fusion Algorithms with Security against Wolves and Lambs in Biometrics", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 2, February 2014, Pages 259-271.
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, Pages 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, Pages 165-180.
7. Cognitive Computational Semantic for high resolution image interpretation using artificial neural network", Biomedical Research.
8. "Cluster based Key Management Authentication in Wireless Bio Sensor Network ", ,International Journal of pharma and bio sciences, Impact Factor = 5.121(Scopus Indexed).
9. Pengye Xia, S.-H. Gary Chan, and Xing Jin, "Optimal Bandwidth Assignment for Multiple-Description-Coded Video", IEEE Transactions on Multimedia, Volume 13, Issue 2, April 2011, Pages 366-375.
10. A Human Computer Interfacing Application ", ,International Journal of pharma and bio sciences.
11. Stefania Colonnese, Francesca Cuomo, and Tommaso Melodia, "An Empirical Model of Multiview Video Coding Efficiency for Wireless Multimedia Sensor Networks", IEEE Transactions on Multimedia, Volume 15, Issue 8, December 2013, Pages 1800-1814.
12. Energy Efficient Two-Phase Sensing for Cooperative Spectrum Sensing in Cognitive Radio Ad hoc Networks"in Central government NISCAIR, Journal of Scientific & Industrial Research (JSIR), New Delhi, india in September 2016 issue.
13. Cuicui Kang, Shiming Xiang, Shengcai Liao, Changsheng Xu, and Chunhong Pan, "Learning Consistent Feature Representation for Cross-Modal Multimedia Retrieval", IEEE Transactions on Multimedia, Volume 17, Issue 3, March 2015, Pages 370-381.
14. Vassil Roussev, Irfan Ahmed, Thomas Sires, "Image-based kernel fingerprinting", Elsevier, Digital Investigation, Volume 11, Issue 2, August 2014, Pages S13–S21.
15. Yijun Yang, Jianping Yu, Peng Zhang, and ShulanWang, "A Fingerprint Encryption Scheme Based on Irreversible Function and Secure Authentication", Hindawi Publishing Corporation, Computational and Mathematical Methods in Medicine, Volume 2015, August 2014, Pages 1-11.
16. 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, Pages 1-14.
17. Kai Cao, Eryun Liu, and Anil K. Jain, "Segmentation and Enhancement of Latent Fingerprints: A Coarse to Fine Ridge Structure Dictionary", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 36, Issue 9, September 2014, Pages 1847-1859.
18. Aisha Azeem, Muhammad Sharif, Mudassar Raza, and Marryam Murtaza, "A Survey: Face Recognition Techniques under Partial Occlusion", The International Arab Journal of Information Technology, Volume 11, Issue1, January 2014, Pages 1-10.
19. Wormhole attacks in mobile ad hoc networks" at National conference Advances in computer, Information and Applied Science on 11th April 2015 organized by Dept of MCA, Sona college of Technology April 2015.
20. Shang-Lin Hsieh, Chun-Che Chen, andWen-Shan Shen, "Combining Digital Watermarking and Fingerprinting Techniques to Identify Copyrights for Color Images", Hindawi Publishing Corporation, Scientific World Journal, Volume 2014, July 2014, Pages 1-15.