Fake Fingerprint Detection Approaches: A Systematic Review

Asraful Syifaa' Ahmad , Rohayanti Hassan, Mohamad Nazir Ahmad

Abstract— Fake fingerprint detection refers to the recognition of a fingerprint image that was created by using a fake fingerprint. These situation are causes the most reliable biometric technology which is fingerprint recognition vulnerable. Therefore, this review presents a collection of the latest literature identified with the fake fingerprint detection and simply center around software-based methodologies. A systematic literature to assessed are performed by examining 146 essential investigations begin with the gross collection of 24 analyze about the papers to decide an scientific categorization, methodologies, on-line open database, and also drawbacks of the fake fingerprint. Besides, 14 techniques focusing in software-methodologies briefly described. Moreover, a few constraints on the fake finger-print images are uncovered and databases that usually utilized by researcher is distinguished. Thus, this review gives an outline of knowledge into the present comprehension of fake fingerprint detection acknowledgement other than distinguishing upcoming research prospects.

Index Terms—Fake fingerprint, fingerprint recognition, liveness detection, LivDet database, systematic literature review

I. INTRODUCTION

Fingerprint has been utilized in scientific (forensic) science and practicesofover100 years [1] and the fingerprint detection area standout among the more broadly used bio-metric advancements. Notwithstanding, analysts found which is present business fingerprint detection systems were helpless and also simple to attacks[2], [3]. To instance, a gathering of German hackers demonstrated to be sidestep the Touch ID security framework on the latest i-Phone 6 following2 days it may dispatch[4]. Moreover, there are likewise a few problems on vulnerability of fingerprint detection with respect to forensics, commercial and the military applications [5]. As per Uludagand Jain [6], there are 2 sorts of attack consist of direct attacks and indirect attacks. While Ratha *et al*. [7] has characterized the attack sto 8of sub-categories according to the available side of the attacks(Figure. 1).

The fake or duplicate finger is utilized on direct attack (Figure. 2). The fake finger is partitioned by 2 sorts that were co-operative and non-cooperative. In the co-operative technique, the theory takes the finger in a Play Doh such as material to making a false impression of the fingerprint has a shape. The shapes are later loaded upto the materials, for example gelatin or silicone which may replicate the unique fingerprint attributes. This can makes purious fake fingerprint. In the non-cooperative sort are utilizing fingerprint images, and a short time later printed on a straight forwardness (transparency) sheet. Additionally, accessible software these days may un doubtedly change over image of the fingerprint to image of an synthetic fingerprint [1], [8].

Subsequently, the fingerprint detection should be able to recognize the live or unique image fingerprint and fake fingerprint images. As indicated by Park *et al*. and Aruna latha and Ezhilarasan[9], [10], the framework must realize how to separate either anspoof or an legitimate finger by guaranteeing that the fingerprint is from a live client. Live-ness recognition depends on the rule that extra data can be accumulated well beyond the information obtained by a standard confirmation (verification) system, and this extra information can be utilized to check if a biometric measure is

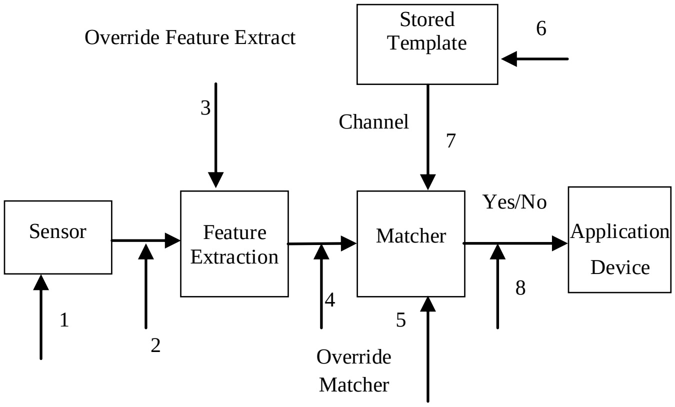

Fig. 1 Eight sub-categories of attack where the number indicates where the attack could happen [7][21] bonafide (valid)[11], [12]

Revised Manuscript Received on March 08, 2019

Asraful Syifaa Ahmad, Faculty of Computing, Universiti Teknologi Malaysia, 81310 Johor Bharu, Malaysia,

Rohayanti Hassan, Faculty of Computing, Universiti Teknologi Malaysia, 81310 Johor Bharu, Malaysia,

Mohamad Nazir Ahmad, Faculty of Computing, Universiti Teknologi Malaysia, 81310 Johor Bharu, Malaysia,

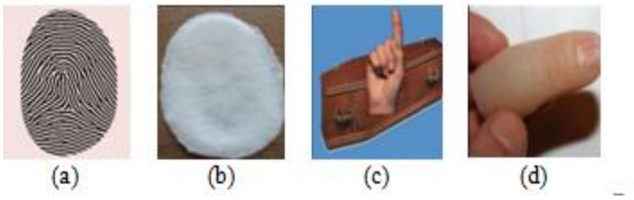

Fig. 2 Example of fake fingerprints. (a) reverse-engineered fingerprint image; (b) 2-D fake fingerprint using Silicone; (c) cadaver fingerprint; (d) synthesized 3-D fake fingerprint [3]

In this way, the survey is done to totally comprehend the properties of fake fingerprint recognize methodology and to recognize any possible area for further research. This paper is composed as follows: Section 2 clarifies the materials and techniques utilized, Section 3 describes the outcome and discussions identified with methodologies.

II. RESEARCH METHODOLOGY

The literature review is biased to induce the unmistakable vision of different fake fingerprint detections which is utilized these days. The targets are to comprehend the properties and outline every one of the methodologies utilized in the detection of a fake fingerprint. To follow the proposal by Achimuguet *al.* [13] and Fieltet *al.* [14] the methodology as proposed in Figure. 3.

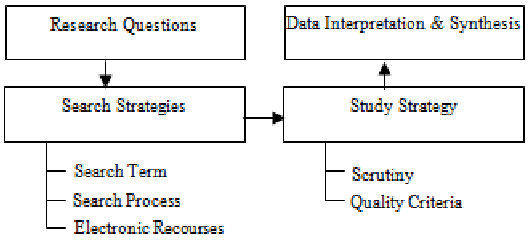

Fig. 3 Research strategy steps

A. Research Questions (RQ)

As the goal of this research is to understand further about current liveness detection approaches, the following research questions were simultaneously explored.

- RQ1: What were the current methodologies in fake fingerprint detection?
- RQ2: What were the descriptions and the non-exclusive (generic) procedure of existing fake fingerprint recognition methodologies?
- RQ3: What were the limitation and problems associated with fake fingerprint recognition?

B. Search Strategies

After constructing the research questions, the search term are maked by utilizing the following steps in Table 1 [13].

Next, by utilizing the search term maked, 3 selected electronic databases are investigated by Scopus (www.scopus.com), IEEE Xplore Digital Library (http:/ieeexplore.ieee.org), and Springer Link (link.springer.com).

Table. 1 Steps of Creating the Search Terms

Steps	Results
To derive the main terms from the research questions.	Fake-Fingerprint-Detection-Approaches
Indicate the synonyms and also alternative spelling	• Fake/False • Fake Fingerprint Detection/Liveness Detection • Approaches/Methods/Software -Based
Integrate the alternative spellings and synonyms, using the Boolean OR and link the major term using Boolean AND	Fake OR false AND Fake Fingerprint Detection OR Liveness Detection AND Approaches OR Methods OR Software-Based

C. Study Selection

All the related papers result from the searched through three selected electronic databases is called as prospective studies [13]or candidates studies [15]. Scrutiny is the process of doing the critical observation. Therefore, all the candidate studies undergo scrutiny studies so that the most relevant to fake fingerprint detection is found. There are several inclusion and exclusion strategy that are utilized to be emphasize the selection of papers. The title and abstract are utilized so as to search the most related papers. Besides that, the selected papers must at least answered either one of the research questions and must be written in the English language. Since the aim is to find the current method, the selected papers must be published from 2013 to 2016. Inclusion and exclusion strategy (criteria)introduced in Table 2 below.

Table. 2 Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Focused on fake fingerprint detection	Not related to fingerprint, fake fingerprint detection and not answer any RQ
Answered at least one RQ	
Written in English language	Not published in English language
Publish year since 2013	No bibliographic information and published on 2012 backwards

D. Data Interpretation and Synthesis

From the main stage, the searching was limited to gather just ongoing studies. Subsequently, one hundred and forty–six (146) potential papers were figured it out. From that point, study selection and scrutiny are done to solution the research questions defined and result in just twenty-four (24) quality papers. At last, the information translation and combination (synthesis) were finished. Those data that related to the first research question (RQ1) are presented using horizontal hierarchical figure. Meanwhile, for RQ2 and RQ3, the data are presented in tables. Along these lines, 7 papers recognized for RQ1 pursued by 14 papers and 7 papers for RQ2 and RQ3 separately. Moreover, this review paper also presented the public online databases that most used by the researchers. The Table below shows the complete list of all the selected papers.

Table. 3 List of Selected Papers

Paper ID	Authors	Year
F1	Galballyet *al.*[16]	2012
F2	Lapsleyet *al.*[17]	1998
F3	Antonelliet *al.*[18]	2006
F4	Baldisserraet *al.*[19]	2006
F5	Kim *et al.*[20]	2016
F6	Park *et al.*[9]	2016
F7	Akhtaret *al.*[21]	2015
F8	Arunalatha and Ezhilarasan[10]	2015
F9	Nogueiraet *al.*[22]	2016
F10	Wang *et al.*[23]	2015
F11	Xia *et al.*[1]	2016
F12	Galballyet *al.*[24]	2014
F13	Kim *et al.*[20]	2016
F14	Bhanarkaret *al.*[25]	2013
F15	Gragnanielloet *al.*[26]	2015
F16	Gragnanielloet *al.*[27]	2013
F17	Dubeyet *al.*[28]	2016
F18	Akhtaret *al.*[29]	2016
F19	Jia *et al.*[30]	2014
F20	Mohammadi and Hariri[31]	2015
F21	Tan and Schuckers[32]	2008
F22	Moonet *al.*[33]	2008
F23	Derakhshaniet *al.*[34]	2003
F24	Abhyankar and Schuckers[35]	2009

III. RESULT AND DISCUSSION

A. Overview

This section present and answered all the research questions. The review result also interpreted in this section.

B. The taxonomy of the approaches (RQ1)

Liveness detection is done not only for fingerprint but also for face and iris. Therefore the fingerprint live-ness detection technique could be isolated into two standard strategies, that is hardware and software. The hardware-based is finished by the sensor for example, identification of fingerprint sweat or blood pressure. It requires extra highlights on the current fingerprint sensor to extract specific features [16]for example, blood pressure [17], skin distortion [18] or scent (odour)[19]. Concurring toKim *et al.*[20], to recognize highlights (features) which separate either live or fake finger the framework need to use extra elements for example, optical coherence tomography scanning systems, oxygen saturation sensors, and also multi-spectral imaging frameworks.

Contrasted with software-based, the image of the fingerprint are utilized as by the component of extraction. Even though the aims is the same software-based are much cheaper and flexible [9]. Throughout the software-based, many researchers had found the solution for the attack of fake fingerprints. Therefore, Akhtar *et al.*[21]Separated the software-based part to 5 sub-categories that is image quality, pores, skin distortion, sweat (perspiration) and combination of variety (Figure 2.).

C. The fake fingerprint detection Methodologies (RQ2)

14 fake fingerprint identification (recognition)methodologies are distinguished from the selected studies. All the data were summarized in the Table 4. Aruna latha and Ezhilarasan[10] proposed a methodology towards the issue in fingerprint detection which dependent on the image quality features. Spatial coherence and clustering factors utilized the edge clarity features, consistency of recurrence field and Gabor features includes by edge (ridge) continuity features within conclusion edge recurrence, differentiate guide, and Direction map for edge strengthening features.

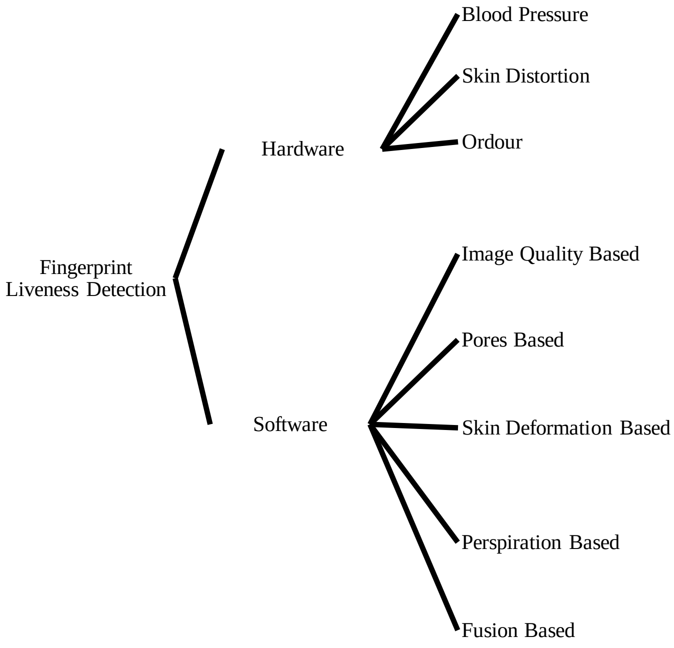

Fig. 4 Taxonomy of fingerprint liveness detection

Nogueiraet *al.*[22] Utilized a kind of feed-forward artificial neural network (ANN), Convolutional Neural Network (CNN) for fingerprint live-ness recognition (detection). The creators thought about for various methods that are (a) CNN (i.e.) pre-prepared on characteristics of natural images, (b) CNN which is fine-tuning with the fingerprint images, (c) CNN with random weights and ultimately (d) an established local binary pattern methodology. The pre-trained CNN may create an better outcome without fine-tuning hyper-parameter choice (selection) or architecture.

Park *et al.*[9] Exhibited an investigation of CNN features of random sample patches to the recognition. The fingerprint images were divided to a few patches utilizing ordinary probability positions. At that point, fake fingerprint is distinguished to utilizing voting strategy on patches grouped by CNN. The CNN were prepared to turning the produced increased patches. The patches amount utilized in this investigation isn't settled. Lower patches additionally can be utilized rather than of all patches in a network.

Wang *et al.*[23]Uncover the non-satisfying after effect of past researchers in utilizing nearby component descriptors for live-ness identification. Accordingly, the creators proposed an answer towards the fake fingerprint problem by utilizing deep convolution neural network (DCNN) and voting methodology in feature selection and classification step. The fingerprint images are sectioned to patches at the least position to anticipate data disturbance of background images. At that point, the voting methodologies are utilized to recombine the patches images to a unique fingerprint image.

Xia *et al.*[1]Examined the technique to identify fake fingerprint by utilizing gradient-based texture features. The creator expressed as two-class classification issue and also utilized the component of co-occurrence array from image gradients to separate features. In the first place, the quantization activity conducted on the images to diminish the dynamic scope of the pixel value. Next, the image gradient is determined on a horizontally and vertically from adjacent quantized pixels. In conclusion from the truncated gradients, the second-order, the third-order of occurrence array, and the components of the co-occurrence clusters were specifically utilized as features.

Galbally*et al.*[24] Presented the low level of complexity detection strategy which improves the security of biometrics detection. It has easy to use, quick, non-intrusive manner, and appropriate for real-time application. The creators' presumptions are that the property of quality image either genuine or fake may be unique. Consequently, the capability of usual image quality evaluation was investigated by the creators by selecting 25 general images quality features. At that point, basic classifiers were joined to recognize within the genuine and fake fingerprint images.

Kim *et al.*[20] Have built up an answer by utilizing deep belief network (DBN). DBN are one of the deep learning methods which may be utilized in some other space. The creators prepared (trained) DBN with numerous layers of Restricted Boltzmann machine (RBM) to group the live or fake fingerprint. The DBN are tried indifferent image from the different kind of sensors and perform effectively and proficiently.

Bhanarkar*et al.*[25]Presented a single-image-based technique has the creators (authors) guarantee which unique fingerprint image of a live individual are not same as from the fake fingerprint image. It is being searched by profiling technique and wavelet-based methodology. To utilizing Daubechies wavelet and to setting the correct threshold, the 2 strategies are acquired. The diverse of these techniques rather than other is, it utilized just only one image without being sectioned.

Gragnaniello*et al.*[26]Uncover, which just broadly useful of nearby descriptor indicates great exhibitions towards fake fingerprint description. In this manner, the creators presented another neighbourhood descriptor for the unique fake fingerprint recognition known by nearby contrast-phase descriptor (LCPD). By utilizing the spatial and recurrence space, the unique fingerprint image is investigated by remove the data of adequacy complexity and neighbourhood behaviour of image. At that point, it has integrated utilizing to change coefficient. Ultimately to recognize it is possible that it fakes or not, the creators utilized support vector machine (SVM) as the classifier.

Gragnaniello*et al.*[27]Displayed, a powerful descriptors for texture classification that is weber local (neighbourhood) descriptor (WLD). WLD demonstrates the better outcome after being tried which a few images from various databases. As per the authors, the combination of WLD and Local Phase Quantization (LPQ) demonstrates a good result than WLD as it were. This methodology is proposed by Weber's Law and comprises of differential excitation and introduction by access every pixels of the fingerprint image.

Dubey*et al.*[28]fuse a few low-level features involving the gradient features from speeded-up robust features (SURF), pyramid histogram of oriented gradients (PHOG) and furthermore the texture features of Gabor wavelet utilizing dynamic score level coordination. Other than, the creators additionally joined to shape investigation to deliver a better outcome. In any case, this technique faced longer computational time analyzes to other people.

Akhtar*et al.*[29]used Partial Least Squares (PLS) to learn correlations in the meantime3 kinds of general classifiers such as Gaussian Mixture Model, Gaussian Copula, and quadratic discriminant analysis (QDA). These 3 kinds of classification are joined to SVM for conclusive classifier.

Jia *et al.*[30]revealed that local binary pattern (LBP) are the better administrator for fake fingerprint recognition. Because of, the authors exhibited multi-scale local binary pattern (MSLBP) to recognize fake fingerprint in both ways. Different ways are used to implement and each of that been combination with a lot of channels. Subsequently, by every example in LBP circle could gather some data from a substantial region rather than a unique pixel.

Mohammadi and Hariri[31]agreed that LBP has the better technique yet it as spatially-constrained and noise-sensitive. Accordingly the authors presented multi-scale centre symmetric local binary pattern (MC-CS-LBP) technique and combination to centre-symmetric local binary pattern for overcome the limitation of original LBP administrator. What

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

more, multi-scale LBP and centre-symmetric LBP connected independently by the image.

D. Limitation of fake fingerprint (RQ3)

In this phase, a few limitations of the fake fingerprint image were uncovered. As indicated byTan and Schuckers[32], fingers create different pressure on the sensor on detection. Because of, live fingerprint takes a reasonable vision of (edge) ridge-valley structure rather than unique fake fingerprint which containing noise. The materials for fake fingerprint had the distinctive elastic characteristics. Hence, different(weight) pressure connected furthermore the revolution of finger on sensor produced distortion. Other than, the (flexible) elastic deformation delivered within the contact of fingertip and plane surface additionally may be utilized has a component which separates within fake and live fingerprint [10]. The deformation are happens when finger contacts the scanner. In any caser, the fake fingerprint has lesser deformation also most it has tends to be distinguished to utilizing different frames of images via clockwise movement of the finger and, cost high computational time [18], [30].

Moon*et al.*[33] Analysed by the elastic behaviour of both fake and live fingerprint by utilizing a numerical method. It was depending on the extraction of the explicitly requested set of minutia points. By and large, the fake fingerprint isn't better in quality contrasted with the genuine unique fingerprint. Next is by utilizing perspiration pores which may be seen in the live unique fingerprint [34]claims that the pores can be caught by utilizing large-resolution scanners and event of pores can be (translated) interpreted utilizing Fast Fourier Transform. Finally, the alternate contrasts of fake and live unique fingerprint known sweat. To utilizing video sequences, perspiring procedure could be estimated as live finger does the sweat procedure[35]. The comparison of the live fingerprint and fake fingerprint were summarized in Table 5.

Table. 4 Summarization of Fake Fingerprint Detection Software Approaches

Features	Methods	Paper ID
Image Quality	Joint Time Frequency Analysis • Profiling the intensity value of original and fake image of fingerprints	F14
	Quality Features • For ridge clarity, author used spatial coherence and clustering factor. • For ridge continuity, author used Gabor features and also uniformity of frequency field • For ridge strength,(edge) ridge frequency, contrast map and direction map are utilized	F8
	Image Quality Assessment • Using 25 general image quality features to differentiate the type of fingerprint images	F12
Gradient-Based Texture	Gradient Intensity and Co-Occurrence Matrix • Image gradient is calculated and used to constructed co-occurrence array and used as features	F11
	Low-Level Features and Shape Analysis • Combine low level features from SURF, PHOG by using integration of score level	F17
Local Descriptor	Multi-Scale Local Binary Pattern • Used MSLBP to overcome the limitation of original LBP • Used LBP histogram comparison to determine the originality	F19
	MS-CS-LBP and MSLBP • Overcome all the limitations of LBP • Apply MS-LBP and CS-LBP separately	F20
	• Partial Least Square • The correlation of fake images and original images is done at first step • Discriminative-generative classification scheme done for spoof detection	F18
	Weber Local Descriptor • Calculate pixels of image using differential excitation and orientation	F16

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

	Local Contrast-Phase Descriptor • Spatial and frequency domain to extract data and behavioral of images the SVM as classifier	F15
Neural Network	Convolutional Neural Network • CNN yield the state-of-art result without any parameter tuning	F9
	CNN Features of Random Sample Patches • Normal probability positions is used to segmented the image • Spoofing detection done by voting strategy and classified by CNN	F6
	Deep Convolution Neural Network • Overcome the limitation of local feature descriptor • Use D-CNN and voting methodology in feature extraction and classification step	F10
	Deep Belief Network • Train DBN with restricted Boltzmann machine to determine either fake or original image	F13

Table. 5 Comparison of Live and Fake Fingerprint

Features	Live Fingerprint	Fake Fingerprint
Ridge valley	Clear	Contain noise
Image quality	Good quality of image	Bad quality
Pores	Exhibit perspiration processes	No pores
Sweat	Sweating process can be measured	No sweat

E. Existing public databases

A few open databases had been utilized by the specialists towards the investigation around there. The most well-known databases are from Live-ness Detection Competition (LivDet). LivDet competition goals to be analyse approach in live-ness recognition by utilizing the expansive quantities of fake and live examples and furthermore standardized testing (convention) rule. This challenge has been facilitated quite a long while and discharges a few databases including LivDet2009, LivDet2011, LiveDet2013 and soon LiveDet2015 [36].

Other than, ATVS databases had additionally been utilized by the analysts. It has included of 4500 genuine and fake dataset which may be utilized to assess the exhibitions in fake fingerprint detection methodology. These fake fingerprint images are gather edage of sticky finger within and without collaboration. 3 unique sensors are utilized that are level optical sensor Biometrika, sweeping thermal sensor by Yubee with Atmel's Fingerchip, and flat capacitive sensor by Precise Biometrics model Precise [37]. Table 6demonstrates databases utilized by every methodology checked on. LivDet2011 and LivDet2009 are referred to and utilized as the state-of-arts or benchmark information in fake fingerprint recognition region

Table. 6 List of Databases used by Each Approach

Technique	Databases	Year	Authors
Convenient Wavelet-Based Algorithm	LivDet2009	2015	Arunalatha and Ezhilarasan
Convolutional Neural Networks	LivDet2009 LivDet2011 LivDet2013	2016	Nogueira*et al.*
Convolutional Neural Networks on random patches	LivDet2009	2016	Park *et al.*
Deep Convolutional Neural Networks Based with Voting Strategy	LivDet2011 LivDet2013	2015	Wang *et al.*
Gradient-Based Texture Features	LivDet2009 LivDet2011	2016	Xia *et al.*
Image Quality Assessment	LivDet2009	2014	Galbally*et al.*
Deep Belief Network Based	LivDet2013	2016	Kim *et al.*
Joint Time Frequency Analysis	-	2013	Bhanarkar*et al.*
Local Contrast Phase Descriptor	LivDet2011	2015	Gragnaniello*et al.*
Weber Local Descriptor	LivDet2009 LivDet2011	2013	Gragnaniello*et al.*
Low-Level Features and Shape Analysis	LivDet2011 LivDet2013	2016	Dubey*et al.*
Partial Least Squares	LivDet2011 LivDet2013	2015	Akhtar*et al.*
Multi-Scale Local Binary Pattern with Filters	LivDet2011	2014	Jia*et al.*
Multi-Scale Center Symmetric Local Binary Pattern	ATVS	2015	Mohammadi and Hariri

IV. CONCLUSION

Systematic literature survey directed is done to comprehend the properties and condense every one of the methodologies utilized in the identification by fake fingerprint. 3 research questions were detailed dependent on the target of investigation. The search procedure through electronic resources, a few search terms are created to facilitate the process. At that point, the study assessment is done by before information synthesis step. This paper surveys late methodologies in fake fingerprints and the description are given. In addition, a few restrictions of fingerprint identification likewise to be expressed in this paper including the (edge) ridge valley, nature of an image, the presence of pores, and sweat. Along these facts, further investigations on fake fingerprint detection approach should possible to dwell on the limitations face looked by biometric recognition. Based on the recent studies, most of the researchers are now focusing on using Neural Network due to the advantages of it. Therefore, in order to develop new optimal fake fingerprint recognition that can cooperate with any type of data from the variety of fingerprint databases, the neural network approaches can be used in the future work.

ACKNOWLEDGMENT

This research is supported by Fundamental Research Grant Scheme (FRGS) and UniversityTeknologi Malaysia under Vote No: 4F744.

REFERENCES

1. Z. Xia, R. Lv, Y. Zhu, P. Ji, H. Sun, and Y. Q. Shi, “Fingerprint liveness detection using gradient-based texture features,” Signal, Image Video Process., vol. 11, pp. 1–8, 2016.
2. A. Al-Ajlan, “Survey on fingerprint liveness detection,” 2013 Int. Work. Biometrics Forensics, 2013, pp. 1–5, 2013.
3. A. Rattani, Z. Akhtar, and G. Foresti, “A preliminary study on identifying fabrication material from fake fingerprint images,” Proc. - 2015 IEEE Symp. Ser. Comput. Intell. SSCI 2015, pp. 362–366, 2016.
4. A. Toosi, S. Cumani, and A. Bottino, “On Multiview Analysis for Fingerprint Liveness Detection,” in Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications: 20th Iberoamerican Congress, CIARP 2015, Montevideo, Uruguay, November 9-12, 2015, Proceedings, A. Pardo and J. Kittler, Eds. Cham: Springer International Publishing, 2015, pp. 143–150.
5. E. Marasco and A. Ross, “A Survey on Antispoofing Schemes for Fingerprint Recognition Systems,” ACM Comput. Surv., vol. 47, no. 2, pp. 1–36, 2014.
6. U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” Proc. SPIE 5306, Secur. Steganography, Watermarking Multimed. Contents, p. 622, 2004.
7. N. K. Ratha, J. H. Connell, and R. M. Bolle, “An Analysis of Minutiae Matching Strength,” Audio- Video-Based Biometric Pers. Authentication, vol. 2091, pp. 223–228, 2001.
8. A. Hadid, N. Evans, S. Marcel, and J. Fierrez, “Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned,” IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, 2015.
9. E. Park, W. Kim, Q. Li, H. Kim, and J. Kim, “Fingerprint liveness detection using CNN features of random sample patches: Liveness detection using CNN features,” Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform., vol. P-260, 2016.
10. G. Arunalatha and M. Ezhilarasan, “Fingerprint Spoof Detection Using Quality Features,” Int. J. Secur. Its Appl., vol. 9, no. 10, pp. 83–94, 2015.
11. V. Mura, F. R. L. Ghiani, G.L. Marcialis, D. A. Yambay, and S. A. S. Clarkson, “Livdet 2015 fingerprint liveness detection competition 2015,” Int. Conf. Biometrics 2013, 2013.
12. L. Ghiani, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, D. Yambay, and S. Schuckers, “LivDet 2013 - Iris Liveness Detection Competition 2013,” Biometrics Theory Appl. Syst., 2013.
13. P. Achimugu, A. Selamat, R. Ibrahim, and M. Naz, “A systematic literature review of software requirements prioritization research,” Inf. Softw. Technol., vol. 56, no. 6, pp. 568–585, 2014.
14. E. Fielt, W. Bandara, S. Miskon, and G. Gable, “Exploring shared services from an is perspective: A literature review and research agenda,” Commun. Assoc. Inf. Syst., vol. 34, no. 1, pp. 1001–1040, 2014.
15. E. D. Madyatmadja and H. Prabowo, “Participation to Public e-Service Development : A Systematic Literature Review,” Int. Conf. Commun. Eng., vol. 8, no. 3, pp. 139–143, 2016.
16. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, “A high performance fingerprint liveness detection method based on quality related features,” Futur. Gener. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.
17. P. Lapsley, J. L. Alexander, D. Pare, and N. Hoffman, “Anti-fraud biometric scanner that accurately detects blood flow,” 1998.
18. A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, “Fake finger detection by skin distortion analysis,” IEEE Trans. Inf. Forensics Secur., vol. 1, no. 3, pp. 360–373, 2006.
19. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, “Fake Fingerprint Detection by Odor Analysis,” Adv. Biometrics, pp. 265–272, 2006.
20. S. Kim, B. Park, B. S. Song, and S. Yang, “Deep belief network based statistical feature learning for fingerprint liveness detection,” Pattern Recognit. Lett., vol. 77, pp. 58–65, 2016.
21. Z. Akhtar, C. Micheloni, and G. L. Foresti, “Biometric Liveness Detection: Challenges and Research Opportunities,” IEEE Secur. Priv., vol. 13, no. 5, pp. 63–72, 2015.
22. R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, “Fingerprint Liveness Detection using Convolutional Networks,” Ieee Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1206–1213, 2016.
23. [23] C. Wang, K. Li, Z. Wu, and Q. Zhao, “A DCNN Based Fingerprint Liveness Detection Algorithm with Voting Strategy,” Springer Int. Publ. Switz. 2015, pp. 241–249, 2015.
24. J. Galbally, S. Marcel, and J. Fierrez, “Image Quality Assessment for Fake Biometric Detection : Application to Iris , Fingerprint , and Face Recognition,” IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, 2014.
25. A. Bhanarkar, P. Doshi, A. Abhyankar, and A. Bang, “Joint time frequency analysis based liveness fingerprint detection,” 2013 IEEE 2nd Int. Conf. Image Inf. Process. IEEE ICIIP 2013, pp. 166–169, 2013.
26. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Local contrast phase descriptor for fingerprint liveness detection,” Pattern Recognit., vol. 48, no. 4, pp. 1046–1054, 2015.
27. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Fingerprint liveness detection based on Weber Local image Descriptor,” 2013 IEEE Work. Biometric Meas. Syst. Secur. Med. Appl. BioMS 2013 - Proc., 2013.
28. R. Dubey, J. Goh, and V. Thing, “Fingerprint Liveness Detection From Single Image Using Low Level Features and Shape Analysis,” IEEE Trans. Inf. Forensics Secur., vol. 6013, no. c, pp. 1–1, 2016.
29. Z. Akhtar, C. Micheloni, and G. L. Foresti, “Correlation Based Fingerprint Liveness Detection,” IEEE, pp. 305–310, 2015.
30. X. Jia, X. Yang, K. Cao, Y. Zang, N. Zhang, R. Dai, X. Zhu, and J. Tian, “Multi-scale local binary pattern with filters for spoof fingerprint detection,” Inf. Sci. (Ny)., vol. 268, pp. 91–102, 2014.
31. S. Mohammadi and M. Hariri, “New Approaches to Fingerprint Authentication Using Software Methods Based on Fingerprint Texture,” in 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), 2015, pp. 1088–1092.
32. B. Tan and S. Schuckers, “New approach for liveness detection in fingerprint scanners based on valley noise analysis,” J. Electron. Imaging, vol. 17, no. 1, p. 11009, 2008.

33. Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, “Wavelet based fingerprint liveness detection,” Trans. Korean Inst. Electr. Eng., vol. 57, no. 6, pp. 982–984, 2008.
34. R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O’Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” Pattern Recognit., vol. 36, no. 2, pp. 383–396, 2003.
35. A. Abhyankar and S. Schuckers, “Integrating a wavelet based perspiration liveness check with fingerprint recognition,” Pattern Recognit., vol. 42, no. 3, pp. 452–464, 2009.
36. “LivDet - Liveness Detection Competitions.” [Online]. Available: http://livdet.org/. [Accessed: 08-Feb-2017].
37. “ATVS - Biometric Recognition Group » Databases » ATVS-FFp.” [Online]. Available: http://atvs.ii.uam.es/ffp_db.html. [Accessed: 08-Feb-2017].
38. Hatim Mohamad Tahir, Emmanuel O.C. Mkpojiogu, “Towards Secure Data Circulation in Mobile Cloud Computing”, International Innovative Research Journal of Engineering and Technology, Vol: 4, Issue: 1, p. 18-23, Sep 2018.