Biometric Security Enhancement Through Dynamic Time Warping-Based Fingerprint Attack Detection

Moreau A.R. & Kim S.T.
Department of Pulmonary Sciences, Bordeaux Clinical Institute, Bordeaux, France
Department of Respiratory Medicine, Incheon Health University, Incheon, South Korea

ABSTRACT

Photo-response non-uniformity (PRNU) of imaging sensors can be employed as a distinctive fingerprint to deal with diverse forensic tasks connecting digital images and video. One of the most significant applications of this knowledge is matching an image or a video snip to the camera that acquired it, which is a task analogous in spirit to matching a shell to a gun cask. The problem examined here distress the condition when an adversary guesstimates the sensor fingerprint from a set of images and applies to it onto an image from a diverse camera to enclose an innocent victim. The previous paper provides a consistent method for detecting such fake fingerprints under quite mild and common assumptions regarding the adversary's movement and the means accessible to the victim. The major drawback of the previous work is that every attack is guessed based on defenders' assumptions. To overcome this, in this paper, we plan to present Dynamic Time Warping (DTW) algorithm to detect sensor finger print. DTW identify similarity among two sequences of finger print images alter in time or speed can be applied to video, audio, and graphics with linear representation. Evaluate an optimal match between two given sequences to detect fake sensor fingerprint at the specific time and event. Sequences are warped non-linearly at the time of fake infusion Utilized with hidden Markov models. Fake Sensor fingerprint detection time is identified exactly by quantifying the similarity variance. Source of Fake generated camera features can be approximately identified. An experimental evaluation is conducted with set of tests in real system to estimate the performance of the proposed DTW to detect sensor finger print contarst with an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification.

Keyword: *Finger print attack, camera identification, Dynamic time warping, hidden markov models.*

I. INTRODUCTION

Fingerprint-based verification is one of the most significant biometric technologies. Human fingerprints are utilized for individual verification in diverse applications and the validity of fingerprint verification has been well defined. Fingerprints are imagined to be distinctive across fingers of similar personality. Even similar twins obtaining similar DNA, are imagined to hold diverse fingerprints. These assumptions lead to the appropriate use of advanced fingerprint based verification in both civilian and law-enforcement applications.

Photo-response non-uniformity (PRNU) of imaging sensors can be utilized as a distinctive fingerprint. While each image taken by a specified sensor includes its PRNU signal, an image can be coordinated to the sensor (camera) by establishing that its noise enduring comprises the similar PRNU. The sensor fingerprint can be expected by averaging noise workings of normal images. Since the fingerprint is fundamentally an arbitrary spread-spectrum signal, it can be noticed using several outline of a matched filter.

Fingerprint matching is one of the most significant methods between biometric verification techniques and has been utilized for person substantiation for a long time. Now, it is not only employed by cornel for law enforcement, but also in ordinary applications, such as process control and financial transmissions. In terms of applications, there are two types of fingerprint substantiation systems: verification and identification. In verification, the given set is a query fingerprint and an identity (ID), the system authorizes whether the ID is reliable with the fingerprint. The outcome is yes or no.

Similarity search among images to identify matches in faces' database utilizing either entire face or particular part of face is a promising feature. Researchers have promoted on such a crisis for the last two decades. Dynamic Time Warping is one of the algorithms that are utilized for time series sequences sorting and similarity measurement. It has high time complexity and low identification accuracy when accessed on images for facial patterns and face identification. Sensor photo-response non-uniformity is a diverse identifier (fingerprint) for forensic tasks E.g., digital-camera ballistics (an image matched to particular camera). Existing work [1] presented fake fingerprint detection under the assumptions on adversary's activity means presentable to the victim by deploying sensor

fingerprint in an image without leaving a trace is more complex. Problem investigated was adversary defined sensor fingerprint from a collection of images superimposes it onto an image from a diverse set of camera (frame an innocent victim). Time of attack initiation and the source unable to identify and similarity variance of the fake fingerprint were made on assumption.

In this paper, we plan to present Dynamic Time Warping (DTW) [8] algorithm to detect sensor finger print. DTW measure similarity between two sequences of finger print images alters in time or speed applied to video, audio, and graphics. Data transformed to linear representation by evaluating an optimal match between two given sequences to detect fake sensor fingerprint at the specific time and event. Sequences are warped non-linearly at the time of fake infusion utilized with hidden Markov models. The main objective of the proposed DTW to detect sensor finger print is that fake sensor fingerprint detection time is identified exactly. Similarity variance is quantified. Faster identification of fake fingerprint.

II. LITEARTURE REVIEW

Fingerprint matching [11] is silent a demanding crisis for consistent person substantiation since of the compound distortions concerned in two impressions of the similar finger. In order to compact with inferior fingerprint images, which commence considerable occlusion and encumber of finer points features [10], we plan a fitness purpose supported on the confined properties of each triplet of finer points. Sensor photo-response non-uniformity [1] has been planned as a distinctive identifier (fingerprint) for different forensic tasks, as well as digital-camera ballistics in which an image is coordinated to a precise camera that took it.

The crisis examined here distress the circumstances when an adversary guess the sensor fingerprint [6] from a deposit of images and overlays it against an image from a diverse camera to structure a naive victim. Since the initiation of this knowledge in 2005, researchers have apprehended that the fingerprint can be imitative onto an image that did not arrive from the camera and thus casing a naive victim. In the most characteristic and quite reasonable situation, Alice, the victim, places her images on the Internet. Eve, the challenger, guess the fingerprint of Alice's camera and correctly overlays it onto another image [3]. Indeed, as previously revealed in the unique publication [2] and, more lately, in [2], threshold-based connection detectors cannot differentiate among an authentic fingerprint and a false one or information fusion [9]. Human action series is also a chronological signal; consequently in [6] the authors engaged DTW to categorize motions from video.

For camera recognition, it is significant that the fingerprint not enclose any other objects (called Non-Unique Artifacts or NUAs in [4]) that might be general transversely sensors/cameras of the similar make since such artifacts are not exclusive to each meticulous sensor and would augment the false alarm. Because most of these artifacts are owing to demosaicking algorithms that depend on the Color Filter Array (CFA) [5] and are interrupted in nature, they can be detached by zero-meaning the rows and columns. A well-informed opponent may, in turn, endeavor to eliminate such artifacts of *C*' and commence interruption artifacts of *C*, for instance, using the technique expressed in [7]. It is now obvious that it is remote from trouble-free to generate a "perfect" forgery.

III. PROPOSED DEFENDING MECHANISM AGAINST FINGER PRINT ATTACK USING DYNAMIC TIME WARPING ALGORITHM

The proposed work is efficiently designed for identifying the finger print copy attack efficiently by implementing the dynamic time warping algorithm to detect the sensor finger print. The dynamic time warping algorithm efficiently determines the similarity among the two sequences of finger print images which varies in time or speed from the camera point of view. The image data from the camera is transformed as a linear representation. The DTW efficiently evaluate an optimal match among the two given sequences of images to detect the fake sensor fingerprint at the specific time and event. In a case of sequences which are warped non-linearly, then the hidden markov models are utilized with the fake infusion. The architecture diagram of the proposed Dynamic Time Warping (DTW) algorithm to detect sensor finger print is show in the fig 3.1.

Warping (DTW) algorithm to detect sensor finger print. At first, the set of sequence fingerprint images are extratced from the dataset and apply the dynamic warping algorithm to identify the similarity among the sequence of finger print images in the set. If the sequence of fingerprint images is linear, the dynamic time warping is used to identify

the fake sensor finger print and if the sequence of fingerprint images is non-linear, hidden markov models are utilized to ensure the similarity among the sequence of fingerprint images in the dataset

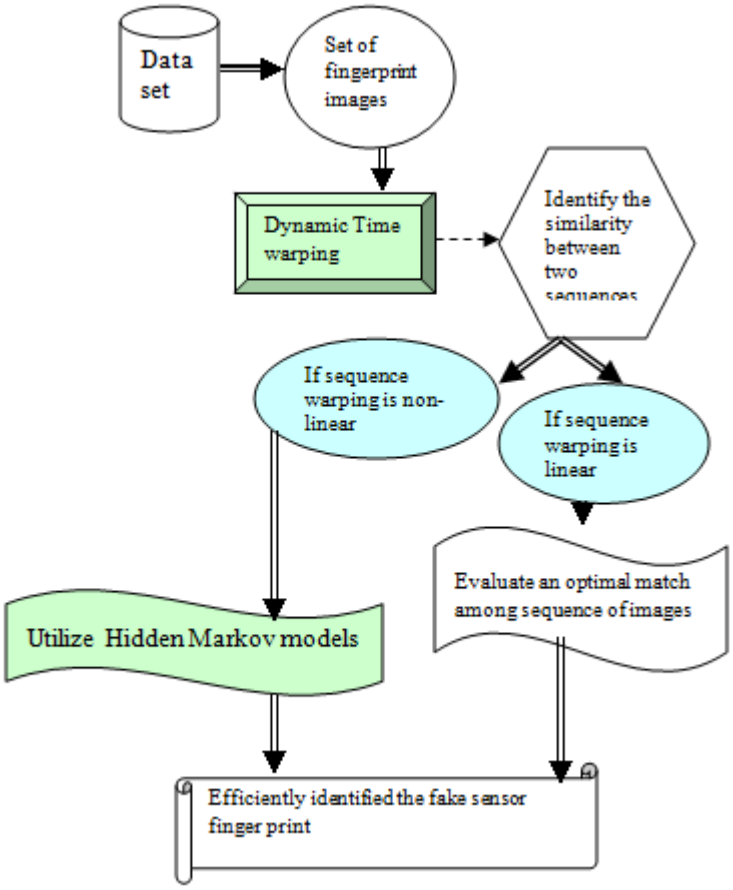

Fig 3.1 Architecture diagram of the proposed proposed Dynamic Time Warping (DTW) algorithm to detect sensor finger print

3.1 Finger print matching problem

For any digital image DI and a denoising filter DF, the noise residual of DI is defined as WI = DI − F (DI). The PRNU signal can be detained employing a multiplicative aspect f, which acting the task of a sensor "fingerprint." Assuming the model, the noise enduring has the form [1]:

$$W_r = aDIf + \Theta \quad \text{..... eqn 1}$$

Where Θ sets for all further noise components, for instance the attempt noise or the announce noise, and '**a'** is a reduction factor of the similar dimension as **f**. In common, 'a**'** depends on the image contented and the dealing out to which DI was subjected to. When representing **Θ** in (2) as an i.i.d. Gaussian, the highest possibility of the PRNU factor **f** from M clatter residuals $W^{(i)} = W_{DI(i)}$ i = 1, …, M, has the form [1]

$$\hat{f} = \frac{\sum_{i=1}^{M} W^{(i)} DI^{(i)}}{\sum_{i=1}^{M} I^{(i)2}} \quad \text{…….. eqn 2}$$

The excellence of the fingerprint estimation is termed as

$$q = corr(f, \hat{f}) \text{ ….. eqn 3}$$

For camera classification, it is significant that the fingerprint not enclose any other objects that might be widespread athwart sensors/cameras of the similar make since such objects are not exceptional to each scrupulous sensor and would augment the false alarm.

By using the finger print features we are capable to hold composite distortions stumbled upon in fingerprint images. Therefore, we can employ a straightforward alteration comprising of scale, revolution and conversion for matching among a template and a query fingerprint in this paper. Assume the positions of finer points in the pattern and the query finger prints are $\{(a_{n,1}, a_{n,2})\}$ and $\{(b_{m,1}, b_{m,2})\}$, correspondingly, where n = 1, 2, 3, . . . , N , m = 1, 2, 3, . . . , M , $(a_{n,1}, a_{n,2})$ and $(b_{m,1}, b_{,2})$ are the coordinates of finer points. The number of finer points in the pattern and the query finger prints are N and M, correspondingly. The alteration $B_i = F(A_i)$ among A_i $(a_{i,1}, a_{i,2})$ and B_i $(b_{i,1}, b_{i,2})$ can be simplified as

$$B_i = s * R * A_i + T \quad \ldots\ldots \text{ eqn 4}$$

where s is the scale factor,

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$T = \begin{pmatrix} T_a \\ T_b \end{pmatrix}$$

is the vector of translation. Consequently, the matching crisis can be termed as to identify the optimized transmission, which can plot as many as probable finer prints in the pattern fingerprint to the minutiae in the query fingerprint.

3.2 Dynamic Time warping algorithm to sensor finger print

DTW algorithm is worked based on active programming techniques. It is employed for measuring similarity among two sequences of fingerprint images which might differ in time or speed. The principle of DTW is to compute two dynamic fingerprints and identify its similarity by evaluating least distance among them.

Dynamic Time Warping is utilized to compute a distance among two sequences of fingerprint images. A series of fingerprint images is a list of sample finger prints taken from a camera, ordered by the time and speed that the respective sample finger prints were obtained. A naive approach to calculating a matching distance between two sequences of finger print images could be to resample one of them and then compare the sequence of fingerprint image sample-by-sample. The drawback of this method is that it does not produce intuitive results, as it compares fingerprint samples that might not correspond well. Dynamic Time Warping provides this inconsistency among perception and considered matching distance by improving finest alignments among section points in the two time series. The configuration is finest in the logic that it reduces a growing detachment measure comprising of "local" distances among associated samples. The process is called *Time Warping* since it distorts the time axes of the two time series in such a way that analogous samples emerge at the similar location on a general time axis.

The DTW-distance among two series of fingerprint images $a_1 \ldots a_M$ and $b_1 \ldots b_N$ is D (M,N), which we compute in a active programming approach using

$$D(i,j) = \min \begin{Bmatrix} D(i, j-1) \\ D(i-1, j) \\ D(i-1, j-1) \end{Bmatrix} + d(a_i, b_i) \quad \ldots. \text{ Eqn 5}$$

The scrupulous alternative of reappearance equation and "local" detachment function d(·, ·) differs with the application. Using the specified three values $D(i-1, j)$, $D(i, j-1)$, and $D(i-1, j-1)$ in the computation of D (i, j) recognizes a *local continuity constraint.*

Then, from each finger print samples, four features per image column are extracted and combined into a single sequence of multi-variate samples. That is, for each finger print image FI with height h and width w, we evaluate an optimal match between two given sequences by extracting a time series X (FI) = $x_1 \ldots x_w$, where each

$$x_i = f_1((FI,i), f_2(FI,i), f_3(FI,i), f_4(FI,i))^T \quad \ldots\ldots\ldots \text{ eqn 6}$$
$$0 \le f_k(.,.) \le 1, k = 1,2,3,4$$

This makes X (FI) a 4-variate vector of length w, where the fk are the four extracted features per image column. In order to run the DTW algorithm on two time series X (FI) and Y (FJ) extracted from images FI and FJ, we have to

define a local distance function that compares the feature sets at aligned columns. We have chosen to use the square of the Euclidean distance:

$$d(x_{fi}, y_{fj}) = \sum_{k=1}^{4} (f_k(FI, i) - f_k(FJ, j))^2 \quad \text{…….. eqn 7}$$

This castigates huge variation among the mined features more greatly than the Euclidean distance would. Now the DTW algorithm can be darted to establish a warping path among X and Y. The length L of the warping path $((i_1, j_1), \ldots, (i_L, j_L))$ biases the determined distance

$$D(X, Y) = \sum_{l=1}^{L} d(x_{i_l}, y_{j_k}) \quad \text{…… eqn 8}$$

The above said actions have been taken place when the sequence of the fingerprint images is linear. DTW identify similarity among two sequences of finger print images change in time or speed and applied to video, audio, and graphics by transforming data to linear representation. Evaluate an optimal match between two given sequences to detect fake sensor fingerprint at the specific time and event.

3.3 HMM for nonlinear sequence of finger print images

Non-linear sequence alignment provides an optimal plotting from the test signal to the pattern signal, whilst permitting a non-linear, monotonic distortion (warping) in the test signal. Hidden Markov models are a structure of stochastic restricted state machine well matched to prototype identification and effectively applied to speech recognition. They are appropriate to the problem pretended here since of their capability to organize patterns supported on a huge quantity of features, whose number is indefinite and which have definite types of primary structure, particularly if that construction results in motionless of the feature distributions over some spatial or temporal period.

Using HMM, the fingerprint identification is done with non-linear representation of data transformed into HMM. HMM typically comprises of extraction, categorization and pretreatment counting noise illumination and exercise progression of HMM engine**.** The process of HMM for analyzing the non-linear sequence of fingerprint is shown in fig 3.2.

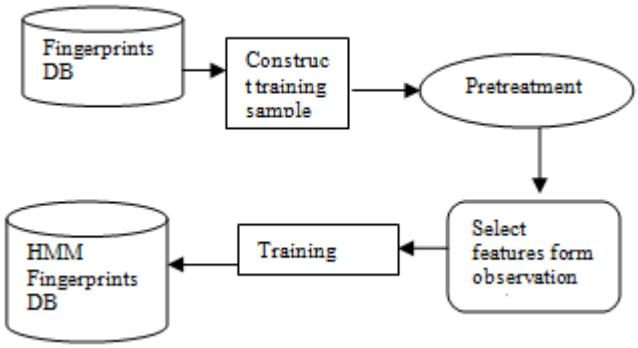

Fig 3.2 Process of HMM

Illustrations from the similar fingerprint communicate to HMM and diverse fingerprints communicate to HMM in HMM DB of fingerprints. The HMM is built by choosing diverse samples of the similar fingerprints with non-linear data representation and employing a training processing, which is a process for guessing the HMM parameters. Fingerprint identification process comprises of a test fingerprint is to discover the utmost matching likelihood of the HMM amongst diverse fingerprints. Because a detained fingerprint emerged arbitrarily in an image, a pretreatment is desirable for regulating the position of a fingerprint and setting the position area, which comprises the complete area for fingerprint identification. Thus the non-linear representation of fingerprint images are pre-treated and the similarity is identified efficiently.

IV. EXPERIMENTAL EVALUATION

The proposed DTW is efficiently designed to perform the detection of sensor fake finger print among the set of finger print images and is implemeted in Java. Methodological analysis and preliminary evaluation have been performed to validate the detection effectiveness on the fingerprint images using DTW for linear warped finger print images and non-linear warped fingerprint images. A real-time approach, specifically for obtaning the fingerprint data and fast response time is achieved by using active detection strategy. A set of tests have been conducted in real system to validate the effectiveness and efficiency of this approach. In the initial phase, Dynamic Time Warping (DTW) algorithm is employed to detect sensor finger print and measured similarity between two sequences of finger print images vary in time or speed. The DTW efficiently evaluate an optimal match between two given sequences to detect fake sensor fingerprint at the specific time and event. If sequences are warped non-linearly at the time of fake infusion, the proposed scheme used with hidden Markov models. Finally, fake Sensor fingerprint detection time is identified exactly. The performance of the proposed DTW to detect sensor finger print is measured in terms of

i) Fake fingerpritnt detection time
ii) Similarity variance
iii) Detection rate

Similarity variance represents the difference between smoothed similarity and its local value, which is equivalent to the high-pass filtered similarity. **I**t indicates local anomalies with respect to the smoothed average background.

V. RESULTS AND DISCUSSION

The proposed defending mechnaism is reliably desgined for identifying the fake sensor fingerprint images by adapting the dynamic time warping method to measure the similarity between two sequences of fingerprint images which are vary in time or speed. If the sequences are warped non-linearly at the time of fake infusion, then the hidden markov models are utilized with it. Comapred to an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification, the proposed DTW to detect sensor fingerprint is reliable in performance. The below table and graph describes the performance of the proposed DTW to detect sensor fingerprint.

Table 5.1 No. of images vs. Fake fingerprint detection time

No. of images	Fake fingerprint detection time (ms)	
	Proposed DTW	Existing DFC
2	1.2	2.5
4	2.4	3.8
6	2.9	4.9
8	3.3	5.6
10	3.7	6.2

The above table (table 5.1) illustrates the time taken to detect the fake fingerprint among the set of fingerprint images. The detection time taken by the proposed DTW to detect sensor fingerprint is compared with an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification (DFC).

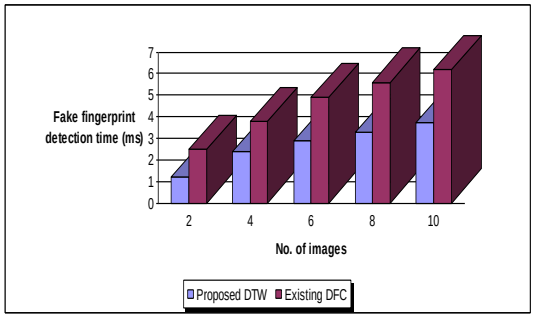

Fig 5.1 No. of images vs. Fake fingerprint detection time

Fig 5.1 depicts the detection time taken to identify the fake fingerprints among the set of fingerprint images taken from the camera sensor device. In the proposed defending scheme, DTW measured similarity between two sequences of finger print images vary in time or speed and it evaluated an optimal match between two given sequences to detect fake sensor fingerprint at the specific time and event. If the sequence of fingerprint imeages are warped non-linearly, the hidden markov models are used to form a sequence set of images and then similariy of images are identified efficiently. The fake fingerprint detection time is measured in terms of milliseconds. Compared to an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification, the proposed DTW to detect sensor fingerprint exaclty identified the fake sensor fingerprint images by consuming less amount of time and the variance is 25-35% low in the proposed DTW.

Table 5.2 No. of images vs. similarity variance

No. of images	Similarity variance	
	Proposed DTW	Existing DFC
1	0.5	0.9
2	0.58	0.79
3	0.63	0.86
4	0.71	0.99
5	0.78	1.2

The above table (table 5.2) illustrates the simialrity variance to detect the fake fingerprint among the set of fingerprint images. The simialrity variance taken by the proposed DTW to detect sensor fingerprint is compared with an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification.

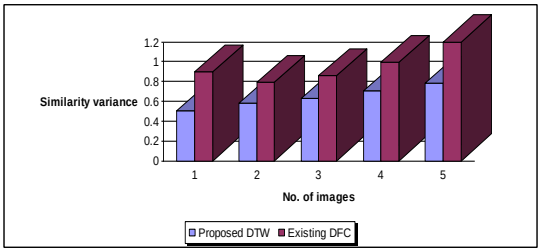

Fig 5.2 No. of images vs. similarity variance

Fig 5.2 illustrates the identification of similarity variance based on the similar sequence of images obtained. The proposed defending mechanism used Dynamic Time warping scheme to defend the simialrity of the sequence of images. Lower the simialrity and higher the varienace leads to the good indicator of sequence of images. Rather than using the triangular scheme for identifying the similarity variance, the proposed defending scheme used DTW and hidden markov models based on the linear and non-linear representation of the fingerprint images. Comapred to an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification, the proposed DTW to detect sensor fingerprint exaclty quantified the simialrity variance by consuming less amount of time and the variance is 20-30% high in the proposed DTW.

Table 5.3 No. of images vs. Fingerprint strength

No. of images	Detection rate (%)	
	Proposed DTW	Existing DFC
2	45	20
4	57	25
6	63	30
8	71	34
10	78	39

The above table (table 5.2) illustrates the fake fingerprint detection rate to detect the fake fingerprint among the set of fingerprint images. The detection time taken by the proposed DTW to detect sensor fingerprint is compared with an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification.

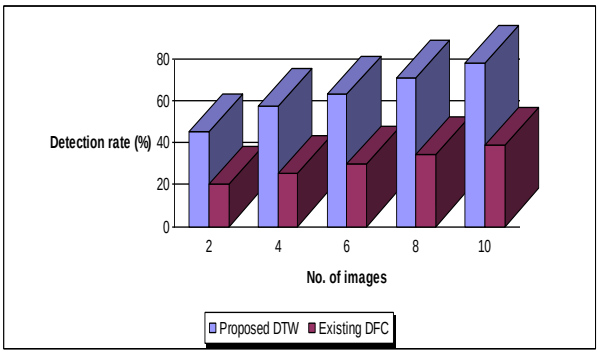

Fig 5.3 No. of images vs. Fingerprint strength

Fig 5.3 illustrates how fast the scheme idetified the fake sensor fingerprint among the set of images. In the proposed defending scheme, DTW measured similarity between two sequences of finger print images vary in time or speed and it evaluated an optimal match between two given sequences to detect fake sensor fingerprint at the specific time and event. If the sequence of fingerprint imeages are warped non-linearly, the hidden markov models are used to form a sequence set of images and then similariy of images are identified efficiently. Compared to an existing Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification, the proposed DTW to detect sensor fingerprint exaclty have faster identification of fake fingerprint and the variance is 30-40% high in the proposed DTW.

Finally, it is being observed that the proposed defending scheme presented Dynamic Time Warping (DTW) algorithm to detect sensor finger print by adapting the similarity between two sequences of finger print images vary in time or speed transformed to linear representation. If the Sequences are warped non-linearly at the time of fake infusion, hidden Markov models is used with it.

VI. CONCLUSION

The proposed defending scheme is effiicently utilized detecting the fake fingerprint sensor identification by presenting Dynamic Time Warping (DTW) algorithm to detect sensor finger print by adapting the similarity between two sequences of finger print images vary in time or speed transformed to linear representation. If the Sequences are warped non-linearly at the time of fake infusion, hidden Markov models is used with it. In the proposed DTW to detect sensor fingerprint, fake sensor fingerprint detection time is identified exactly and the similarity variance is also being quantified. The fake fingerprint is identified in a reliable manner and the source of fake generated camera features can be approximately identified. An experimental evaluation has been carrie dout to prove the performance and effectiveness of the proposed defending mechanism used to detect the fake fingerprint among the set of fingerprint images and reliable in terms of detection time, rate, similarity variance.

REFERENCE

1. *Miroslav Goljan et. Al., " Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification", IEEE Transactions on Information Forensics and Security, March 2011*
2. *Steinebach, M., Liu, H., Fan, P., Katzenbeisser, S.: "Cell phone camera ballistics: attacks and countermeasures," Proc. SPIE, Multimedia on Mobile Devices 2010, SPIE, vol. 7542, pp. 0B–0C, 2010.*
3. *Chen, M., Fridrich, J., Goljan, M., and Lukáš, J.: "Determining Image Origin and Integrity Using Sensor Noise." IEEE Transactions on Information Security and Forensics 1(1), pp. 74–90, March 2008.*
4. *Goljan, M.: "Digital Camera Identification from Images – Estimating False Acceptance Probability," Lecture Notes in Computer Science, Digital Watermarking, vol. 5450, Proc. IWDW08, Busan, South Korea, pp. 454–468, 2009.*

5. *Bloy, G. J.: "Blind Camera Fingerprinting and Image Clustering." IEEE Transactions on Pattern Analysis and Machine Intelligence 30(3), pp. 532–534, March, 2008.*
6. *Rosenfeld, K. and Sencar, H. T.: "A Study of the Robustness of PRNU-Based Camera Identification." Proc. SPIE, Media Forensics and Security XI, vol. 7254, San Jose, CA, January 18–22, pp. 0M–0N, 2009.*
7. *Xuejun Tan, Bir Bhanu, "Fingerprint matching by genetic algorithms", Pattern Recognition 39 (2006) 465 – 477*
8. *Kevin Adistambha et'al, "Motion Classification Using Dynamic Time Warping", International Workshop on Multimedia Signal Processing 2008.*
9. *O. Ali and N. Cristianini. Information fusion for entity matching in unstructured data. In Artificial Intelligence Applications and Innovations, volume 339 of IFIP Advances in Information and Communication Technology, pages 162–169. Springer Boston, 2010.*
10. *Böhme, R. and Kirchner, M.: "Synthesis of Color Filter Array Pattern in Digital Images." Proc. SPIE, Media Forensics and Security XI, vol. 7254, San Jose, CA, January 18–22, pp. 0K–0L, 2009.*
11. *Goljan, M., Fridrich, J., and Filler, T.: "Large Scale Test of Sensor Fingerprint Camera Identification." Proc. SPIE, Media Forensics and Security XI, vol. 7254, San Jose, CA, January 18–22, pp. 0I–0J, 2009.*