Minutiae Based Fingerprint Image Hashing

Rajesh Muthu
Faculty of Engineering and Environment
Northumbria University,
Newcastle upon Tyne, UK.
rajesh.muthu@northumbria.ac.uk

Ahmed Bouridane
Faculty of Engineering and Environment
Northumbria University,
Newcastle upon Tyne, UK
ahmed.bouridane@northumbria.ac.uk

Fouad Khelifi
Faculty of Engineering and Environment
Northumbria University,
Newcastle upon Tyne, UK.
fouad.khelifi@northumbria.ac.uk

***Abstract*— This paper proposes a robust minutiae based fingerprint image hashing technique. The idea is to incorporate the orientation and descriptor in the minutiae of fingerprint images using SIFT-Harris feature points. A recent shape context based perceptual hashing method has been compared against the proposed technique. Experimentally, the proposed technique has been shown to deliver better robustness against image processing operations including JPEG lossy compression and geometric attacks such as rotation and translation.**

***Keywords*— Minutiae; feature extraction; shape contexts; fingerprint image hashing.**

I. Introduction

Fingerprint-based recognition is the oldest serving, most successful and popular method as a person identification system. Fingerprints consist of a regular texture pattern composed of ridges and valleys. In a fingerprint the focused feature points are the minutiae. i.e., ridge endings and ridge bifurcation[1]. The spatial distribution of these minutiae points are claimed to be unique for each finger and therefore, the collection of minutiae points in a fingerprint is primarily employed for matching two fingerprints. A good quality of fingerprint consists of between 20 to 70 minutiae [2], all of which are not genuineness and prominence.

Recently, many researchers have addressed the hashing of fingerprint minutiae. In [3] [4], the authors present a method of symmetric hashing of fingerprint minutiae, aimed to protect the original fingerprint and minutiae location from the attacker. In [5], the authors proposed a scheme which employs a robust one–way transformation that maps geometrical configuration of the minutiae points into a fixed-length code vector. In [6], the authors describe a template privacy protection technique for the minutiae cylinder code (MCC). This provides diversity, revocability, and irreversibility for MCC descriptors with respect to the original minutiae to improve the recognition accuracy and reduces the template size. In [7], the authors proposed a locality-sensitive hashing (LSH) based fingerprint indexing using reduced SIFT points. Xu, Haiyun, et al [8], approached the spectral minutiae representation as a fixed- length feature vector to represent the minutiae set.

Most countermeasures proposed in the literature generally focus on feature extraction to get robust feature to authenticate the images. In [9], the authors present a method for feature transforms, as it transforms image data into scale invariant coordinates relative to local features. In [10], the authors present an image hashing algorithm using visually significant feature points and performed a performance and tradeoffs evaluation between geometric invariance and robustness against classical attacks. In [11], the authors presented a fast performance scale and rotation invariant interest point detector and descriptor coined SURF (Speeded-Up Robust Feature). In [12], the authors developed a new image hashing algorithm using robust local feature point, introducing SIFT-Harris detector to select the most stable SIFT keypoints which are less vulnerable to image processing attacks.

In this paper, we propose a method for extracting the robust minutiae of fingerprint image, by combining SIFT-Harris feature points with minutiae of fingerprint images, as illustrated in Fig. 1. The idea is to incorporate the orientation and descriptor in the minutiae of fingerprint image. In our proposed approach, shape context based hashing [12] is used for fingerprint identification. Shape contexts provide an excellent description of the geometric structure of a shape. We can embed the geometric distribution of robust minutiae feature points as well as their descriptors into a short hash vector. The rest of the paper is structured as follows. Section II describes the feature extraction and the proposed robust minutiae extraction of fingerprint image. Sections III provide a shape contexts based hashing. Section IV presents experimental result and analysis in comparison with related techniques. Section V concludes the paper.

II. Feature Extraction

A. Fingerprint Minutiae Extraction

Many Automatic Fingerprint Identification Systems (AFIS) are based on minutiae matching. A minutiae based fingerprint recognition system undergoes three main stages, namely pre-processing, minutiae extraction and post- processing [1][13]. Pre-processing stage consists of image enhancement, image binarization, Image segmentation. Thinning and minutiae marking is done at the minutiae extraction stage and finally, the removal of false minutiae in post-processing stage. Fig2. shows minutiae extraction of the fingerprint image.

978-1-4799-6773-5/14/$31.00 ©2014 IEEE

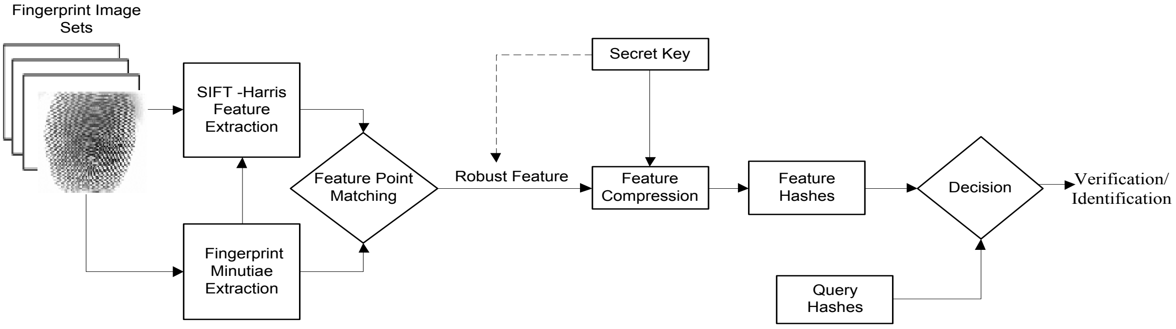


Fig 1: Proposed Robust Fingerprint Image Hashing

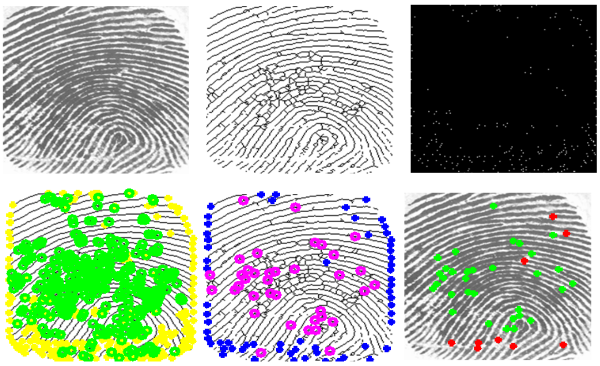


Fig 2: Minutiae Extraction of the fingerprint image

B. *SIFT- Harris Feature Extraction*

A local feature is an image pattern which differs from its immediate neighborhood. It is usually associated with a change in an image property such as intensity, color and texture.

1)Scale Invariant Feature Transform[9][12]: Scale invariant local points are detected by searching for local extrema in the series of difference-of-Gaussian (DoG) image. The DoG is constructed by the convolution of a variable scale Gaussian function $G(x,y,\sigma)$,with an image $I(x,y)$ in the scale space of an image $L(x,y,\sigma)$.

$$D(x,y,\sigma) \approx (k-1)\sigma^2\nabla^2 G * I(x,y) \quad (1)$$
$$= (k-1)\sigma^2 G * \nabla^2 I(x,y) \quad (2)$$

Where $\nabla^2 I(x,y)$ is Laplacian operator, used to detect edges and corners in an image. Based on the scale, position and orientation of each keypoint, the corresponding descriptor having 128 points based on the gradient histogram within its 16x16 local neighborhood is generated.

2) Harris Detector: DoG detector of SIFT provides satisfying performance under geometric transforms. Its robustness against attacks, like additive noise and blurring, is poor. To extract robust local features, it is desired to select the most stable keypoints under various distortions and attacks. Harris corner [14] could provides stable detection performance with high repeatability and localization accuracy under various distortion and geometric transformations. Therefore, the Harris criterion is incorporated to select the most stable SIFT keypoints.

The Harris detector/criterion to evaluate the corner points is

$$H = \lambda_1\lambda_2 - k(\lambda_1+\lambda_2)^2 = \det(\mathrm{M}) - ktrace^2(\mathrm{M}) \quad (3)$$

Where λ_1, λ_2 are eigenvalues of autocorrelation matrix M and k is a coefficient ranging 0.04 - 0.015.

Given set of SIFT points $= \{p_i(x,y,\sigma,\theta)\}_{i=1}^N$, where x and y are coordinates and σ, θ are scale and orientation parameters, respectively. $H_i^\sigma(x,y)$ is Harris response and σ the standard deviation of the Gaussian kernel window used to compute the auto-correlation matrix M, set the threshold T to select robust SIFT point as

$$T = \frac{\alpha}{N}\sum_{i=1}^{N} H_i^\sigma(x,y) \quad (5)$$

Where α is an adjustable parameter to control the robust points selection and empirically α ∈ [0.1,0.5].

C. *Proposed Robust Minutiae of Fingerprint Images.*

To design a robust fingerprint hashing against various distortions, robust feature extraction is the most important step. We propose a method for extracting the robust minutiae of fingerprint images, by combining SIFT-Harris feature points with minutiae of fingerprint image, as shown in Fig. 1. Based on the position, scale, and orientation of each key point in SIFT-Harris, the corresponding descriptor with 128 dimensions based on the gradient histogram within its 16x16 local neighborhood is generated. Alongside SIFT-Harris feature points ($\mathrm{SH_{FP}}$), minutiae ($\mathrm{M_P}$) are extracted with four tuple, such as $\mathrm{M_P}=\{\mathrm{x,y},\theta,\mathrm{t}\}$, where, (x,y) is the coordinate, θ is angle, and t is the type of minutiae (termination or bifurcation) respectively. The absolute radial distance between the position of SIFT-Harris feature and the coordinate of minutiae are computed. Most robust minutiae are detected if the relative difference of pixel values is within the threshold of ten pixel value. Along with the detected point the corresponding orientation and descriptor are also identified. The proposed robust minutiae are represented by coordinates, orientation and descriptor respectively. This robust minutiae of fingerprint image is to be hashed, and the fingerprint identification is to be performed using hashed robust minutiae. The detailed hashing technique is explained in section 3.

The robustness of the image hashing arises from robust feature extraction and the compression which mainly contributes to the compactness of the final hash. To increase the security of a traditional hash function and prevent unauthorized access, a secret key is incorporated at either the feature extraction, compression or both to make the hashes unpredictable. Most of the hashing algorithms incorporate a pseudorandomization relying on a secret key. Such a keying is incorporated into the compression step[10][12], to further enhance the security as indicated by the dashed line in fig 1. The key is owned by the owner, the hash generation is a pseudorandom process rather than a completely random one for fingerprint identification. The incoming query hash corresponding to the query image is compared with the hashes in the database.

III. SHAPE CONTEXT BASED HASHING

In our proposed approach, shape context based hashing [12] is used for fingerprint identification. Shape contexts provide an excellent description of the geometric structure of a shape. We can embed the geometric distribution of robust feature points as well as their descriptors into shape contexts to generate a compact image hash. The original shape context was designed to be computed for each point sampled from the object contours, which means that for N local feature points we have N shape contexts. It provides a rich descriptor to represent the shapes, but has to be compressed to be used for hashing directly.

It is observed in image content identification and authentication that all perceptually insignificant distortions and malicious manipulations on the image content would not lead to viewpoint changes, the center of an image is generally preserved and relatively stable under certain geometric attacks. This motivates Xudong and Jane Wang [12] to generate shape contexts with the reference point in the center and obtain a compact signature for the image. Another reason for avoiding computing shape context for each local feature point in hashing is that keypoints detection cannot guarantee to yield exactly the same feature points when the image is under different attacks and manipulations. As a trade-off, we use radial shape context hashing (RSCH) and angular shape context hashing (ASCH), to generate hashes using shape contexts with respect to the central reference point.

Given a set of local key points $P = \{p_i(x,y)\}_{i=1}^{N}$and their corresponding local descriptors $D = d_{pi}(\text{x},\text{y})\}_{i=1}^{N}$, the basic steps of RSCH and ASCH are as follows [12]:

A. Radial Shape Context Hashing (RSCH)

1. Given the coordinates of the central point C =$(x_c$,$y_c)$ and the required length of the hash L, construct bins $B = \{b(k)\}_{k=1}^{N}$ of shape contexts with incremental l =max$(x_c$,$y_c)/$L in radial direction of polar coordinates.

$$b(k) = \{p_i \in P: (k-1)l \leq [\![p_i - C]\!] \leq kl\} \qquad (6)$$

Where $[\![p_i - C]\!]$ is the relative distance between pi and the central point C.

2. Generate pseudorandom weights $\{\propto_k\}_{k=1}^{L}$ from the normal distribution N(u,σ^2) using a secret key. Each $\propto_k$ is a random vector with 128 dimensions to be consistent with dimension of SIFT descriptors.

3. Let $H = \{h_k\}_{k=1}^{L}$ be the hash vector, we have each component h_k as

$$h_k = \sum_{p_i \in b(k)} w_{[L\Delta\theta_{pi}/2\pi]} \langle \propto_k d_{pi} \rangle \qquad (7)$$

Where $\Delta\theta_{pi}$= $(\theta_{pi} - \theta_c) \in (0,2\pi)$ is the relative difference of orientations between p_i and the central point C.The weight w $[L\Delta\theta_{pi}/\ 2\pi] \in W = \{w_i\}_{i=1}^{L}$, is the set of random weights generated from uniform distribution U(0.5,1). This is to differentiate the points located at different orientations of the same hash bin $b(k)$ along the radial direction.

B. Angular Shape Context Hashing (ASCH)

1. Given the coordinates of the central point C=$(x_c$,$y_c)$ and the required length of the hash L, construct bins $B = \{b(k)\}_{k=1}^{N}$ of shape contexts with incremental $l = 2\pi/$L in angular direction of polar coordinates .

$$b(k) = \{p_i \in P: (k-1)l \leq (\theta_{pi} - \theta_c) \leq kl\} \qquad (8)$$

Where $(\theta_{pi} - \theta_c)$ =$\Delta\theta_{pi} \in (0,2\pi)$.

2. Generate pseudorandom weights from the normal distribution N(u,σ^2) using a secret key. Each $\propto_k$ is a random vector with 128 dimensions to be consistent with the dimension of SIFT descriptors.

3. Let $H = \{h_k\}_{k=1}^{L}$ be the hash vector, we have each component h_k as

$$h_k = \sum_{p_i \in b(k)} w_{[L\|p_i - C\|/\|C\|]} \langle \propto_k d_{pi} \rangle \qquad (9)$$

Where $\|P_i - C\|$ is the same as mentioned in section 3A and $\|C\|$ =$\sqrt{x_c^2 + y_c^2}$ is the normalization factor. The weight $w_{[L\|P_i - C\|/\|C\|]} \in W = \{w_i\}_{i=1}^{L}$, is the set of random weights generated from uniform distribution U(0.5,1). This is to differentiate the points located at different orientations of the same hash bin $b(k)$ along the angular direction.

Estimation of Central Orientation θ_C: Radon transform to estimate an accurate reference orientation of central point C. The Radon transform of $f\ (x, y)$ is the integral of orthogonal projection to line p

$$R_f\ (\text{p},\theta)=\int_{-\infty}^{\infty} f(x,y)dq \qquad (10)$$

Where q is the orthogonal axis of line p.

$$x = pcos\theta - qsin\theta \qquad (11)$$

$$y = psin\theta + qcos\theta \qquad (12)$$

IV. EXPERIMENTAL RESULT AND ANALYSIS

In this work, we chose the following two metrics for characterizing the robustness and discriminability of the perceptual hashing scheme. These are Euclidean distance and Receiver Operating Characteristics (ROC).

A. Euclidean Distance

Let $S = \{s_i\}_{i=1}^{N}$ be the set of original images in the database. The corresponding hashes space $\text{H(S)} = \{\text{H}(\text{s}_\text{i})\}_{\text{i}=1}^{\text{N}}$, Where H (s_i) = { $h_1(s_i), h_2(s_i), \ldots \ldots \ldots h_3(s_i)$} is the hash vector with length n for image s_i. We use Euclidean distance D$((h_1),(h_2))$ to measure the similarity between two hash vectors H(s_1) and H(s_2). Given a query image Q, generate its hash H(Q) and calculate its distance to each original image in the hash space H(S).The distance between two hashes is defined as the square root of the sum of the squares of the differences between the corresponding hash values. i.e., the distance between two hashes h_1 *and* , h_2 is given by

$$dist\big((h_1),(h_2)\big) = \sqrt{\sum_{i=1} \left(h_{1_i} - h_{2_i}\right)^2} \qquad (13)$$

B. Receiver Operating Characteristics (ROC)

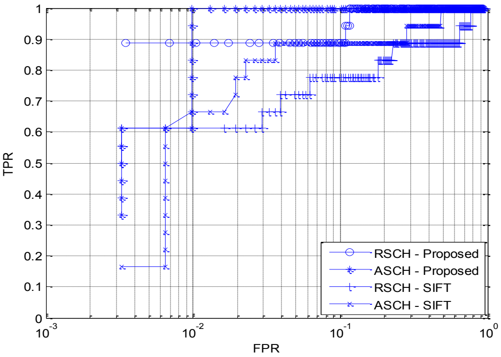
ROC Curve is used to evaluate the identification performance of the proposed robust minutiae based fingerprint image hashing technique. To plot ROC curve, we compute and store the hash values for the original image, denoted as h_1 and its attacked version as h_2. If the Euclidean distance between hashes $dist(h_1, h_2) < Th,$ we declare it as authentic, where Th is a decision threshold, referred to here as TPR (True Positive Rate). For visually different images, denoted as h_3, the Euclidean distance between hashed $dist(h_1, h_3) < Th,$ and are referred to as FPR (False Positive Rate). ROC curve is the plot TPR against FPR, recommends that the best possible performance would correspond to the upper left corner of the ROC space.

C. Result and Analysis

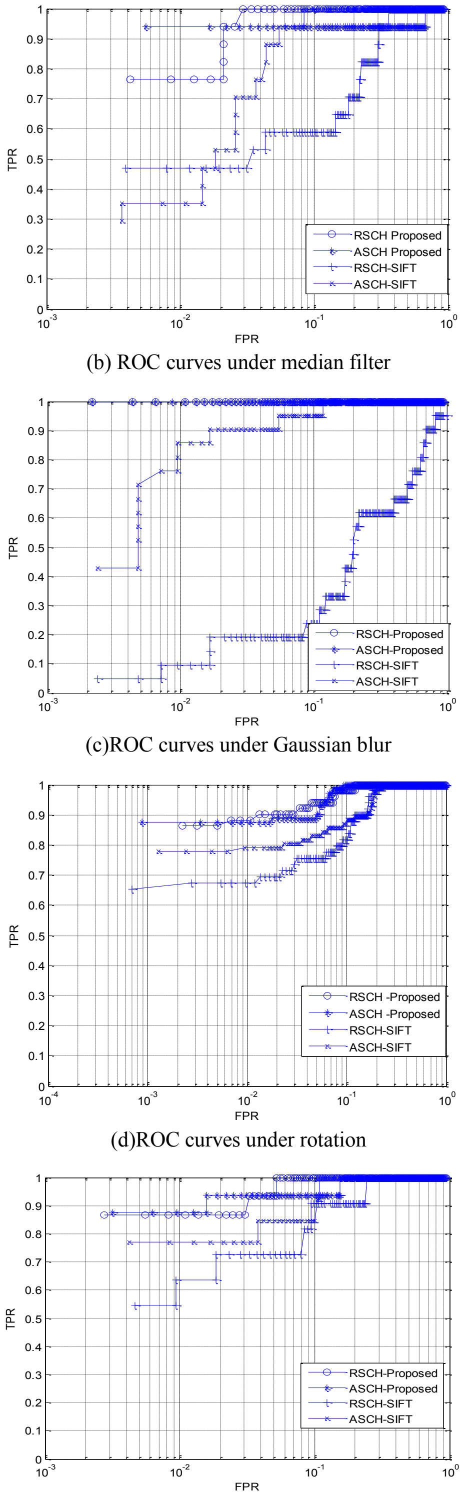
The proposed technique was evaluated using 100 images in the FVC 2002 database. We evaluated the perceptual robustness of the image hashing techniques, RSCH and ASCH against the known attacks as mentioned in Table1. The selected length of the hash vector of RSCH and ASCH is L=20[12]. The proposed robust feature extraction of fingerprint images has been compared with SIFT technique, as shown in fig 3(a-e); The results show that the proposed robust minutiae of fingerprint image hashing technique has been shown to deliver better robustness against known image processing and geometric operations. The advantage of generating hashes based on the robust minutiae of fingerprint image lies in the robustness against geometric distortions like rotations and translations. The hashing technique RSCH and ASCH performs better for identification accuracy. We have observed that Angular shape context hashing relatively outperforms Radial shape context hashing, indicating that the distribution of feature points in the angular direction is better discriminated than in the radial direction.

Table 1: Different Attacks used to assess the hashing performance

Attack	Parameters
Image Processing JPEG lossy compression Median Filter Gaussian Blur	 Quality Factor =10 3x3 window 3x3window
Geometric Distortion Rotation Translation	 5^0 σ =0.5,5x5 window



(a) ROC curves under JPEG lossy compression



(b) ROC curves under median filter

(c)ROC curves under Gaussian blur

(d)ROC curves under rotation

(e) ROC curves under translation

Fig 3: ROC curves of the proposed robust minutiae of fingerprint image using shape context based image hashing technique, (a) ROC curves under JPEG lossy compression (b) ROC curves under median filter (c) ROC curves under Gaussian blur (d) ROC curves under rotation (e) ROC curves under translation.

V. CONCLUSION

In this paper, we have developed robust minutiae based fingerprint image hashing. Based on the geometric invariance of SIFT-Harris keypoints, we combined the minutiae of fingerprint with SIFT-Harris feature to detect robust minutiae. We incorporate the orientation and descriptor in the minutiae of fingerprint image. Fingerprint identification is performed using hashed robust minutiae. Shape contexts provide an outstanding description of the geometric structure of a shape. We can embed the geometric distribution of robust minutiae feature points as well as their descriptors into a short hash vector. Therefore, SIFT-Harris-Minutiae is more suitable for generating template and for the comparison of the fingerprint content.

REFERENCES

[1] Bouridane, Ahmed. *Imaging for Forensics and Security: From Theory to Practice*. Vol. 106. Springer, 2009.

[2] Jain,Anil K, J.Feng and K.Nandakumar, "Fingerprint Matching", *IEEE Computer*, Vol. 43, No. 2, pp. 36-44, February 2010.

[3] Tulyakov, S, Farooq,F and Govindaraju, V. "Symmetric hash functions for fingerprint minutiae." *Pattern Recognition and Image Analysis*. Springer Berlin Heidelberg, 2005. 30-38.

[4] Tulyakov, S., Farooq, F., Mansukhani, P., and Govindaraju, V "Symmetric hash functions for secure fingerprint biometric systems." *Pattern Recognition Letters* 28.16 (2007): 2427-2436.

[5] Sutcu, Yagiz, Husrev T. Sencar, and Nasir Memon. "A geometric transformation to protect minutiae-based fingerprint templates." *Defense and Security Symposium*. International Society for Optics and Photonics, 2007.

[6] Mirmohamadsadeghi, Leila, and Andrzej Drygajlo. "A template privacy protection scheme for fingerprint minutiae descriptors." *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the*. IEEE, 2013.

[7] Shuai, Xin, Chao Zhang, and Pengwei Hao. "Fingerprint indexing based on composite set of reduced SIFT features." *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*. IEEE, 2008.

[8] Xu, H., Veldhuis, R., Bazen, A. M., Kevenaar, T. A., Akkermans, T. A., & Gokberk, B. "Fingerprint verification using spectral minutiae representations." *Information Forensics and Security, IEEE Transactions on* 4.3 (2009): 397-409.

[9] Lowe, David G. "Distinctive image features from scale-invariant keypoints." *International Journal of computer vision* 60.2 (2004): 91-110 .

[10] Monga, Vishal, and Brian L. Evans. "Perceptual image hashing via feature points: performance evaluation and tradeoffs." *Image Processing, IEEE Transactions on* 15.11 (2006): 3452-3465.

[11] Bay, Herbert, Tinne Tuytelaars, and Luc Van Gool. "Surf: Speeded up robust features." *Computer Vision–ECCV 2006*. Springer Berlin Heidelberg, 2006. 404-417.

[12] Lv, Xudong, and Z. Jane Wang. "Perceptual image hashing based on shape contexts and local feature points." *Information Forensics and Security, IEEE Transactions on* 7.3 (2012): 1081-1093.

[13] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." *Circuits and Systems for Video Technology, IEEE Transactions on* 14.1 (2004): 4-20.

[14] Harris, Chris, and Mike Stephens. "A combined corner and edge detector." *Alvey Vision Conference*. Vol. 15. 1988.