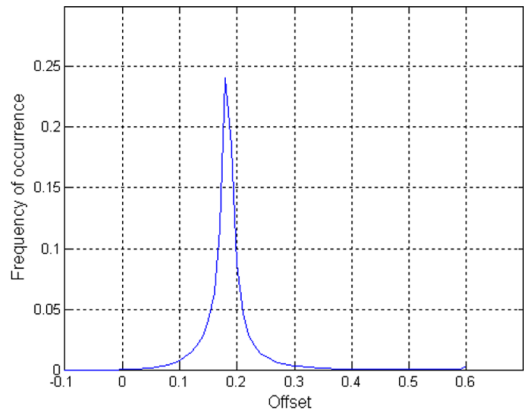

Fig. 3. Offset of the modulus of negative real zeroes caused by one gray-scale value change.

is shown in Fig. 2(e) and we can observe that the tampered area was accurately detected.

B. Fragility of Watermark to Pixel Perturbation

From our observation, the zero locations of the z-transform are very sensitive to the value change of even a single pixel, which renders the z-transform domain ideal for fragile watermarking. We have investigated this property experimentally. We collected 1000 gray-scale natural images and calculated the negative real zeroes of the z-transform of their pixel sequences as described in Section III. We then randomly changed one pixel value in every sequence and calculated the amplitudes of the offsets of the negative real zeroes, which are reported in Fig. 3. It can be observed that even a single pixel's change unavoidably disturbs the zero locations. In addition, we found that 98% of the negative real zeroes tend to shift toward the unit circle and as illustrated in Fig. 3, the distribution peaks at an offset of 0.18, which is enough to change the watermark detection results.

V. Conclusion

In this paper, we discuss a novel fragile watermarking method based on the z-transform domain. The watermark bits are embedded by slight perturbation of the zero locations. The zeroes of the z-transform around the unit circle are very sensitive to any change of the host image. This important property provides the scheme with special sensitivity to any alteration to the watermarked image and the ability of accurate localizing. In addition, the proposed method is more secure than normal fragile watermarking techniques based on LSB embedding. Simulation results confirmed the applicability of the proposed algorithm.

References

[1] C.-S. Lu and M. H.-Y. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[2] A. T. S. Ho, X. Zhu, and Y. L. Guan, "Image content authentication using pinned sine transform," *EURASIP J. Appl. Signal Process., Special Issue Multimedia Security Rights Manag.*, vol. 2004, no. 14, pp. 2174–2184, Oct. 2004.

[3] M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proc. Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997, vol. 2, pp. 680–683.

[4] P. W. Wong, "A watermark for image integrity and ownership verification," presented at the IS & T PIC Conf., Portland, OR, May 1998.

[5] P. W. Wong, "A public key watermark for image verification and authentication," in *Proc. IEEE Int. Conf. Image Processing*, 1998, vol. 1, pp. 455–459.

[6] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.*, vol. 11, no. 6, pp. 585–595, Jun. 2002.

[7] X. Zhang and S. Wang, "Statistical fragile watermarking capable of locating individual tampered pixels," *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 727–730, Oct. 2007.

[8] E. C. Ifeachor and B. W. Jervis, *Digital Signal Processing: A Practical Approach*. Wokingham, U.K.: Addison-Wesley, 1993.

[9] R. H. T. Bates, B. K. Quek, and C. R. Parker, "Some implications of zero sheets for blind deconvolution and phase retrieval," *J. Opt. Soc. Amer. A, Opt. Image Sci.*., vol. 7, no. 3, pp. 468–479, Mar. 1990.

[10] R. Vich, *z-Transform Theory and Applications*. Dordrecht, The Netherlands: Reidel, 1987.

# On the Assumption of Equal Contributions in Fingerprinting

Hans Georg Schaathun

***Abstract*—With a digital fingerprinting scheme, a vendor of digital copies of copyrighted material marks each individual copy with a unique fingerprint. If an illegal copy appears, it can be traced back to one or more guilty pirates due to this fingerprint. A coalition of pirates may combine their copies to produce an unauthorized copy with a false, hybrid fingerprint. It is often assumed in the literature that the members of the collusion will make equal contributions to the hybrid fingerprint, because nobody will accept an increased risk of being caught. We argue that no such assumption is valid *a priori*, and we show that a published solution by Sebé and Domingo–Ferrer can be broken by breaking the assumption.**

***Index Terms*—Collusion-attack, collusion-secure code (CSC), digital fingerprinting, scattering codes.**

I. Background

The problem of digital fingerprinting was introduced in [1] and has received quite some attention following [2]. A vendor of digital copies of copyrighted material wants to prevent unauthorized copying. Digital fingerprinting makes it possible to trace the guilty user (pirate) when an illegal copy is found. This is done by embedding a secret identification mark (fingerprint) in each copy, making every copy unique.

Typically, a robust watermarking (WM) scheme is used to hide the fingerprint in the file. WM schemes are designed to hide any message in a file in such a way that they can be recovered, even after being subject to noise, signal-processing operations, or even malicious attacks.

If a single pirate distributes unauthorized copies, they will carry his or her fingerprint. If the vendor discovers the illegal copies, he or she can trace them back to the pirate and prosecute him or her. However, a collusion of users can compare their copies, and thereby find regions

Manuscript received July 28, 2007; revised May 8, 2008. This work was supported in part by the Norwegian Research Council under Grant 146874/420, conducted under employment with the University of Bergen, Norway. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Upamanyu Madhow.

The author is with the Department of Computing, University of Surrey, Guildford GU2 7XH, U.K. (e-mail: h.schaathun@surrey.ac.uk).

Digital Object Identifier 10.1109/TIFS.2008.926991

which differ and, hence, must be part of the fingerprint. A simple attack is to cut and paste segments from their individual copies, to produce a hybrid copy where the fingerprint does not match any of the colluders.

Many authors [3], [4] assume that a collusion will always make a hybrid by combining equal shares from each of their fingerprints. This is based on the idea that the more the user fingerprint resembles the hybrid, the more likely the user is to be accused. Obviously, nobody would accept a higher risk of being accused.

The assumption may be correct when the closest neighbor or correlation decoding is used [3] but, in general, it is not valid. Obviously, if we prove that the system is secure assuming a certain user behavior, then we are sure that a malicious (and intelligent) user will find some other behavior. This is illustrated by the scattering codes [5], and we shall prove that they are indeed not secure when the users are not restricted to equal contributions.

The purpose of this paper is to highlight how important it is in information security and not to jump to conclusions about user behavior. Any statement about user behavior must be demonstrated based on the actual system.

II. Collusion-Secure Codes

A common model for fingerprinting combines a WM scheme with a collusion-secure code (CSC) [3]. An $(n, M)_q$ code C is a set of M words $(c_1, \ldots, c_n)$ over a q-ary alphabet Q. Each user is associated with a fingerprint (word) $\mathbf{c} \in C$. The file is divided into n segments, and each symbol c_i is embedded independently in a corresponding segment.

The code C is often viewed as an $n \times M$ matrix called the codebook, where the rows are codewords. Each column corresponds to a segment of the file.

A collusion of t pirates will have a set $\mathcal{P} \subseteq \mathcal{C}$ of fingerprints. We will also think of $\mathcal{P}$ as an $n \times t$ matrix, and refer to columns of $\mathcal{P}$. A column i, $1 \leq i \leq n$, is detectable if more than one element of Q occurs in column i of $\mathcal{P}$. We will assume that the correspondence between file segments and code columns is chosen pseudorandomly by the vendor and kept secret [6]. Hence, the colluders have no means of knowing which columns they detect.

By comparing their copies, the pirates are able to produce an unauthorized copy with a hybrid fingerprint $\mathbf{x} \in Q^n$. The pirates choose an attack function $A : Q^{n \times t} \to Q^n$, possibly stochastic, taking the pirate fingerprints $\mathcal{P}$ as input and returning the hybrid fingerprint $\mathbf{x}$.

The set of hybrid fingerprints producible by P is called the feasible set $F_{\mathcal{C}}(\mathcal{P})$. This restricts the attack function, so that $A(\mathcal{P}) \in F_{\mathcal{C}}(\mathcal{P})$. The most common model due to [2] assumes that

$$F_{\mathcal{C}}(\mathcal{P}) = \{(c_1, \ldots, c_n) : \forall\, i,\ \exists\, (x_1, \ldots, x_n) \in \mathcal{P}, x_i = c_i\}.$$

In other words, each symbol x_i in the hybrid fingerprint $\mathbf{x}$ must occur in the ith column of $\mathcal{P}$. This is known as the marking assumption.

A tracing algorithm for the code $\mathcal{C}$ is any algorithm $T : Q^n \to \{L : L \subseteq C\}$. The input is the hybrid fingerprint $\mathbf{x}$ from an unauthorized copy, and the output L is a list of users who are accused of copyright violation. If $\mathcal{P}$ is a set of pirate fingerprints and A is an attack function producing $\mathbf{x} = A(\mathcal{P})$, then T is successful if $L \subseteq \mathcal{P}$ and $L \neq \emptyset$. If T is not successful, we say that there is an error. A (probabilistically) CSC is one with a tracing algorithm with bounded error probability.

III. Scattering Codes (SC)

Scattering codes were introduced in [5] and [7] and used in conjunction with a simplex code to give a probabilistically three-secure code. An alleged attack [8] was rebutted in [6].

The scattering code $\mathrm{SC}(r, t)$ is a probabilistic encoding of a single bit. Each bit value is encoded as one out of t possible words, chosen uniformly at random. The code has $2t+1$ distinct columns replicated r times. We divide the columns into three zones. Zone A has r identical columns where a word has one if and only if it encodes one. Zone B has t distinct columns of weight one replicated r times, and all words encoding zero are zero. Zone C is similar, with t distinct columns of weight 1, and words encoding one are zero. Table I gives an example.

TABLE I
Scattering Code $\mathrm{SC}(4, 3)$

Encodes	Zone A	Zone B	Zone C
1	1111	1111 0000 0000	0000 0000 0000
	1111	0000 1111 0000	0000 0000 0000
	1111	0000 0000 1111	0000 0000 0000
0	0000	0000 0000 0000	1111 0000 0000
	0000	0000 0000 0000	0000 1111 0000
	0000	0000 0000 0000	0000 0000 1111

TABLE II
Three Pirate Codewords

A	B_1	B_2	B_3	C_1	C_2	C_3
r bits	r bits	r bits	r bits	r bits	r bits	r bits
1111	1111	0000	0000	0000	0000	0000
1111	0000	1111	0000	0000	0000	0000
0000	0000	0000	0000	1111	0000	0000

As part of the embedding, the fingerprint is XORed with a random, secret bit string $\mathbf{k}$. Similarly, the extracted hybrid fingerprint is XORed with $\mathbf{k}$ before descattering. The effect of this is that the colluders cannot tell whether a segment hides a 0 or a 1; they can only tell whether two segments are different. (This randomization prevents the attack from [8].)

Assuming that we detect a hybrid fingerprint produced by three colluders, the following decoding algorithm aims to recover a symbol seen by at least two of the colluders.

Algorithm 1 (Descattering [5]): The decoding algorithm for scattering codes (descattering) uses the first applicable rule in the following list. One block is one set of r identical columns.

1) If there are at least two blocks of Zone B with at least one one-bit, then decode as 1.
2) If there are at least two blocks of Zone C with at least one one-bit, then decode as 0.
3) If there are more ones than zeroes in Zone A, then decode as 1.
4) If there are more zeroes than ones in Zone A, then decode as 0.
5) With the same number of zeroes and ones in Zone A, decode as erasure.

It is easy to validate that the algorithm is always correct if the rows of $\mathcal{P}$ encode the same bit. Table II shows a typical example where the collusion sees two different bits. We can see that if the pirates use a minority choice strategy with high probability, they will probably output at least one one-bit in each B_1 and B_2, and decoding rule 1 will cause decoding to 1. If they use a majority choice strategy with high probability, they are likely to produce a majority of ones in block A, and cause correct decoding of 1 by Rule 3. In the lemma as will be shown, we will establish the exact probability of correct decoding.

In [7], attacks were considered where the colluders make independent, random choices for each segment. We describe the strategy as a tuple (p_1, p_2, p_3) where p_i is the probability that the attack outputs the bit seen by two colluders (majority choice) in a column where colluder no. i differs from the other two. Due to the assumption of equal contributions, [7] assumed $p_1 = p_2 = p_3$. The following lemma is a generalization of a result from [5] and [7]. The proof is a trivial extension of the original, but is included for completeness.

Lemma 1: Let $\mathbf{a}_1$, $\mathbf{a}_2$, and $\mathbf{a}_3$ be three codewords held by the collusion, where $\mathbf{a}_i$ encodes the opposite value of the other two codewords.

Suppose the pirates pick the majority bit with probability p_j in any column where user j is the minority. Then, the probability of correct descattering r_i is given as

$$r_i = 1 - \frac{1 + (t-1)\left(\sum_{j \neq i} p_j^r - \prod_{j \neq i} p_j^r\right)}{t} \sum_{j=0}^{\lfloor r/2 \rfloor} \binom{r}{j} p_i^j (1-p_i)^{r-j}.$$

Proof: We prove the lemma for $i = 3$, assuming that $\mathbf{a}_3$ encodes a 0. The general case follows by symmetry.

We consider first the case where $\mathbf{a}_1 \neq \mathbf{a}_2$. Suppose the pirate codewords are as depicted in Table II. In order to obtain a decoding error, both Rule 1 and 3 have to fail. The first rule fails if least one of Block B_1 and B_2 is all zero, and this occurs with probability

$$P_1 = p_1^r + p_2^r - p_1^r p_2^r.$$

The other rule fails if Zone A has a majority of zeros, which occurs with probability

$$P_3 = \sum_{j=0}^{\lfloor r/2 \rfloor} \binom{r}{j} p_3^i (1-p_3)^{r-j}.$$

The two events are independent, so the error probability is $P_1 \cdot P_3$.

If $\mathbf{a}_1 = \mathbf{a}_2$, there is only one block Zone B, say B_1, where the pirates see two different bits. Hence, decoding Rule 1 always fails, and we have a decoding error with probability P_3.

For each bit, one of the t codewords is chosen uniformly at random. Hence, $P(\mathbf{a}_1 = \mathbf{a}_2) = 1/t$, and we obtain the following total error probability:

$$P_E = P_3 \cdot \frac{(t-1)P_1 + 1}{t}$$

which is equivalent to the formula in the theorem. Note that the error probability increases in p_1 and p_2 and decreases in p_3. ∎

If $p_1 = p_2 = p_3 =: p$, then clearly $r_1 = r_2 = r_3 =: \rho(p)$ by symmetry. The worst-case probability of successful descattering $p^*(r,t) := \min_p \rho(p)$ is calculated in [5].

In [5], a scattering code S was concatenated with a simplex code C as an outer code. In other words, each user was represented by a binary codeword $\mathbf{c} \in C$, and each bit of $\mathbf{c}$ was encoded using S. The decoder would first descatter block by block, and then decode the resulting vector with respect to C using closest neighbor decoding. It was proved that if the descattering is successful with sufficiently high probability, then the error probability of the outer decoding can be made arbitrarily close to 0. As we shall see, this result is only valid for strategies (p,p,p).

Remark 1: Closest neighbor decoding invariably returns one and only one codeword which is accused. There is no distinction between false negatives and false positives. An error means that the returned user is innocent, and both a false positive and a false negative are implied. If the returned user is guilty, we say that decoding is correct, but there are still two unidentified members of the collusion (false negatives).

We can view the outer code as a fingerprinting code in itself. For a column of C where colluder i has a fingerprint different from the other two, we can define a probability r_i that the resulting hybrid fingerprint after descattering matches the other two colluders. This is the probability r_i given in Lemma 1. In effect, we obtain a colluder strategy (r_1, r_2, r_3) with respect to the outer code.

Theorem 1: A fingerprinting scheme with scattering inner codes and a linear outer code has an error rate of at least 1/4 if the pirates use an optimal strategy, regardless of the outer decoding algorithm used.

TABLE III
EXAMPLE OF THE STRATEGIES IN THE PROOF OF THEOREM 1

	Strategy			
Innocent user	(111)	(001)	(010)	(100)
$\mathbf{c}_1 = (1000)$	(0110)	(0000)	(1100)	(1010)
$\mathbf{c}_2 = (0100)$	(1010)	(0000)	(1100)	(0110)
$\mathbf{c}_3 = (0010)$	(1100)	(0000)	(1010)	(0110)
$\mathbf{c}_4 = (1110)$	(0000)	(1100)	(1010)	(0110)

In particular, the simplex code C is linear. In the case of list decoding, an error rate of 25% means that, on average, 25% of all accused codewords are false positives.

Proof: We propose a mixed strategy where the colluders choose a pure strategy (p_1, p_2, p_3) uniformly at random from $\{(1,1,1),(1,0,0),(0,1,0),(0,0,1)\}$. Observe that each of these four strategies gives $(r_1, r_2, r_3) = (p_1, p_2, p_3)$.

Consider three linearly independent codewords $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$, and $\mathbf{c}_4 = \mathbf{c}_1 + \mathbf{c}_2 + \mathbf{c}_3$. By linearity, $\mathbf{c}_4 \in C$. Any collusion of three out of these four codewords by using our proposed strategy will produce the same four false fingerprints with equal probabilities. Hence, when one of these false fingerprints is detected, there are four users who are equally likely to be guilty and one of them is innocent. ∎

Example 1: Table III shows an example of the strategies used in the proof. Since the attack works independently on each column, we have truncated the codewords to display each column type (up to equivalence) once. The first column shows the four codewords, and each row then shows the four hybrid words generated when the corresponding user is innocent (by the other three codewords). Note that each codeword that the decoder can observe appears once in each row. Consequently, any one of the four users may be innocent.

Remark 2: The problem with the original construction is clearly in the outer code. Our attack only works because the outer code is linear. It was proved in [9] and [10] that a secure construction can be made by using a nonlinear outer code (so-called $(2,2)$- and $(3,1)$-separating codes). Unfortunately, the rate of such a code is inferior to other codes in the literature and, therefore, we have omitted the details.

IV. CLOSING WORDS

We conclude that the fingerprinting code of [7] is broken if the colluders refuse to accept the assumption of equal contributions, and an optimal attack gives an error rate of at least 25%. This proves that the assumption of equal contributions is not valid in general, and it is worrisome that this assumption is so often accepted in the literature (e.g., [4]) without argument.

It is an open question to check the assumption for other proposed solutions where it has been applied. In many cases, it can almost certainly be proved that an optimal attack exists where equal contributions are used, but then this would be a property of the particular fingerprinting scheme and not of the fingerprinting model.

REFERENCES

[1] N. R. Wagner, "Fingerprinting," in *Proc. Symp. Security Privacy*, 1983, pp. 18–22.
[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.
[3] M. Wu, W. Trappe, Z. J. Wang, and K. J. R. Liu, "Collusion resistant fingerprinting for multimedia," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 15–27, Mar. 2004.
[4] S. He and M. Wu, "Joint coding and embedding techniques for multimedia fingerprinting," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 231–248, Jun. 2006.
[5] F. Sebé and J. Domingo-Ferrer, "Short 3-secure fingerprinting codes for copyright protection," in *Proc. ACISP*, 2002, vol. 2384, pp. 316–327.

[6] F. Sebé and J. Domingo-Ferrer, "Critique to Burmester and le attack on Sebé and Dommingo-Ferrer fingerprinting scheme," *Electron. Lett.*, vol. 40, Sep. 2004.
[7] F. Sebé and J. Domingo-Ferrer, "Scattering codes to implement short 3-secure fingerprinting for copyright protection," *Electron. Lett.*, vol. 38, pp. 958–959, Aug. 2002.
[8] M. Burmester and T. Le, "Attack on Sebé, Dommingo-Ferrer and Herrera-Joancomarti fingerprinting schemes," *Electron. Lett.*, vol. 40, Feb. 2004.
[9] H. G. Schaathun, "Fighting three pirates with scattering codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2004, p. 202.
[10] H. G. Schaathun, "Fighting three pirates with scattering codes," Dept. Inf., Univ. Bergen, Bergen, Norway, 2004. [Online]. Available: http://www.ii.uib.no/~georg/sci/inf/coding/public/.

A Selective Feature Information Approach for Iris Image-Quality Measure

Craig Belcher and Yingzi Du

***Abstract*—Poor quality images can significantly affect the accuracy of iris-recognition systems because they do not have enough feature information. However, existing quality measures have focused on parameters or factors other than feature information. The quality of feature available for measure is a combination of the distinctiveness of the iris region and the amount of iris region available. Some irises may only have a small area of changing patterns. Due to this, the proposed approach automatically selects the portions of the iris with the most distinguishable changing patterns to measure the feature information. The combination of occlusion and dilation determines the amount of iris region available and is considered in the proposed quality measure. The quality score is the fused result of the feature information score, the occlusion score, and the dilation score. The relationship between the quality score and recognition accuracy is evaluated using 2-D Gabor and 1-D Log-Gabor wavelet approaches and validated using a diverse data set. In addition, the proposed method is compared with the convolution matrix, spectrum energy, and Mexican hat wavelet methods. These three methods represent a variety of approaches for iris-quality measure. The experimental results show that the proposed quality score is highly correlated with the recognition accuracy and is capable of predicting the recognition results.**

***Index Terms*—Biometrics, feature information, iris-quality measure, iris recognition.**

I. Introduction

POOR quality images can significantly reduce the accuracy of iris-recognition systems [1]–[13]. It has been shown that the performance of iris-recognition systems can be improved when quality is considered [2], [3], [5], [7]. Many factors can affect the quality of an iris image, including defocus, motion blur, occlusion, dilation, glare, resolution, image contrast, and iris deformation. Noncooperative iris-recognition systems are more susceptible to quality problems, but even cooperative systems can capture iris images of varying quality that are affected by these quality problems. Some quality methods have been adapted to improve the quality of acquired iris images [2] in the hardware level. These approaches are good for quickly eliminating very poor quality images, but even images capable of accurate segmentation can be assigned varying levels of quality as some iris images are naturally more discriminating than others.

Daugman [2] analyzed the optical defocus model and proposed an 8×8 convolution kernel to fast assess the focus of an iris image. It acts as a bandpass filter. Ma *et al.* [7] used the frequency energy distribution of two iris subregions in the horizontal direction to measure the image quality. The support vector machine (SVM) was used to classify the images into two categories (good and bad) based on low–, middle-, and high-frequency energy levels. Chen *et al.* [5] divided the entire iris region into eight concentric bands and measured the frequency content using a Mexican hat wavelet. The quality score of the entire iris image is the weighted average of the quality scores of individual bands. The bands closer to the pupil are given a higher weight. This approach has good spatial adaptivity based on local image quality [5]. Kalka *et al.* [6] proposed using the Dempster–Shafer theory to combine several quality measures, including defocus, motion blur, occlusion, specular reflection, lighting, off angle, and pixel counts. This method improves over other methods by using multiple parameters, and the defocus quality measure uses Daugman's 8×8 convolution matrix in the iris region. Other quality measures include Zhang and Salganicoff's sharpness measure for focus [10] and Zhu *et al.*'s iris texture analysis [11].

Poor quality images cannot generate satisfactory recognition because they do not have enough feature information, which has not been well considered in these quality measures. Iris recognition is dependent on the amount of information available in two iris images being compared. The quality of feature available for measure is a combination of the distinctiveness of the iris region and the amount of iris region available.

In [12], we proposed the clarity measure by comparing the information loss from the original features to blurred versions of the same features. This approach can only work on iris images with a small amount of occlusion. In addition, it is very sensitive to segmentation error.

In this paper, we propose a selective feature information approach for iris-quality measure that evaluates the available distinctive feature information. The experimental results show that the proposed quality measure is highly correlated with the recognition accuracy. Therefore, it can be used to determine the confidence level of matching scores. When two images are compared, it is possible for two low-quality images to have a high matching score and be from different eyes or have a low matching score and be from the same eye. A confidence score can be used to support matching results by allowing a system to only focus on matching scores that meet some confidence level. Two iris-recognition algorithms are used to evaluate the proposed quality measure: 2-D Gabor wavelet method proposed by Daugman [2] and 1-D Log-Gabor wavelet method proposed by Masek and Kovesi [14] with our improvement [18]. The proposed method is compared with other methods [2], [5], [7] over three public databases: 1) CASIA ver. 2.0 [15]; 2) ICE 2005 [16]; and 3) the West Virginia University (WVU) database [23]. The experimental results show that the proposed method is effective.

II. Selective Feature Information-Based Iris Image-Quality Measure

A. Preprocessing

The acquired iris image includes pupil, eyelids, eyelashes, sclera, and some skin of the eye as well as iris. The first step is to preprocess

Manuscript received September 10, 2007; revised April 4, 2008. This work was supported in part by the ONR Young Investigator Program under Award N00014-07-1-0788 and in part by the National Institute of Justice under Award 2007-DE-BX-K182. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Anil Jain.

The authors are with the Electrical and Computer Engineering Department, Indiana University–Purdue University, Indianapolis, IN 46202 USA (e-mail: yidu@iupui.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2008.924606