

Protecting Digital Fingerprint in Automated Fingerprint Identification System using Local Binary Pattern Operator

K. Ait sadi¹, I. Bouchair¹, K. Zebbiche² and M. Laadjel²

¹ Centre de Développement des Technologies Avancées, Division Architecture des Systèmes,
Cité 20 Août 1956, BP 17, Baba Hassen, 16303, Algier, Algeria

² Centre de Recherche et Développement de la Gendarmerie Nationale, (CRD-GN), Algier, Algeria
aitsaadi@cdta.dz, CRD.CGN@mdn.dz

Keywords: Fingerprint, LBP, Arnold Scrambling, Watermarking, AFIS System.

Abstract: The Local binary pattern (LBP) operators, which measure the local contrast within a pixel's neighbourhood, have been successfully applied to texture analysis, face recognition, and image retrieval. In the paper, we present a new application of the LBP operators for securing digital fingerprint in AFIS System (Automated Fingerprint Identification System), while inserting a robust watermark (ID image and Face image) to increase not only security but also to facilitate the recognition of the person. To improve the security of the embedding, the watermarks are scrambled using Arnold technique and are then hidden in the fingerprint image of the corresponding person. Experimental results show that the proposed watermarking method is robust against commonly-used image processing operations, such as additive noise, luminance change, contrast enhancement, and JPEG compression while does not change the fingerprint features and maintains a good visibility of the original fingerprint images.

1 INTRODUCTION

Biometric systems based on fingerprints as AFIS systems developed by the Federal Bureau of Investigation (FBI) and other agencies and researchers aim to identify persons from their fingerprints previously acquired and stored in the data base system. However, Due to their popular use in many applications, these systems are not immune from errors and attacks that attempt to exploit vulnerabilities to destabilize their performance. Uludag, et al. (Uludag and Jain, 2004) identify eight basic sources of attacks that are possible in a generic biometric system (Figure 1). In the first type of attack, a false biometric (such as a fake finger) is presented at the sensor. Resubmission of digitally stored biometric data constitutes the second type of attack. In the third type of attack, the feature detector could be forced to produce feature values chosen by the attacker, instead of the actual values generated from the data obtained from the sensor. In the fourth type of attack, the features extracted using the data obtained from the sensor are replaced with a synthetic feature set. In the fifth type of attack, the matcher component could be attacked to produce high or low matching scores, regardless of the input

feature set. Attack on the templates stored in databases is the sixth type of attack. In the seventh type of attack, the channel between the database and matcher could be compromised to alter transferred template information. The final type of attack includes altering the matching result itself. All of these attacks have the possibility to decrease the credibility of a biometric system. Several techniques based on digital watermarking and data hiding have been proposed in the literature to enhance biometric security against the aforementioned attacks.

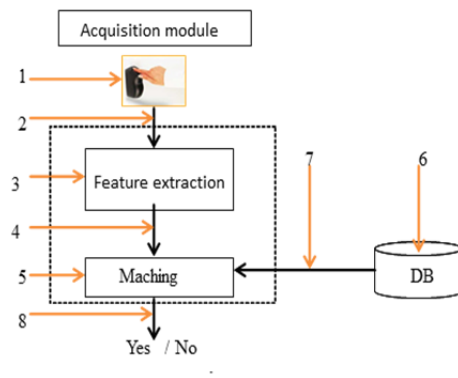


Figure 1: The different points of attack on the AFIS system (Uludag and Jain, 2004).

Pravin et al. in (Pravin et al., 2011) proposed a stegano-crypto system for enhancing biometric feature security with RSA and data hiding. The aim is to increase security of biometric system and facilitate identification. They used a biometric code generated from captured biometric image. The light of this paper is the use of the RSA algorithm and data hiding process to protect the biometric information against attacks. But the authors did not precise whose is the biometric image used as host image and those used as watermarks. Also the authors did not investigate about the robustness of the data hiding against attacks and distortion inducted with watermark embedding. Thus, because sometimes the embedding destroys the biometric features of biometric image itself. For example, when the face features are embedded into fingerprint image, the features of fingerprint may get disturbed and wrong minutiae points may arise. Another point important is that the authors did not discuss the credibility of the verification and recognition performance under attacks

Jain et al. (Jain and Uludag, 2003) have hidden fingerprint image features in face image. Then they proposed to hide the facial information as watermark to authenticate the fingerprint image. A bit stream of eigenface coefficients is embedded into selected fingerprint image pixels using a randomly generated secret key. The extraction bits are then employed for fusion recognition with host fingerprint image. However, since the Extracted pattern is given for identification without credibility verification, it only increases recognition performance under attack free circumstances thus provide no additional security. Another important criterion to respect in the data hiding is the payload which is low in the proposed algorithm.

Mathivadhani et al. (Mathivadhani and Meena, 2010) have presented a comparative study on fingerprint protection using watermarking techniques. However, most of these works induced distortion with watermark embedding sometimes destroys the biometric features of the fingerprint image itself. For example, when the face features are embedded into fingerprint image, the features of fingerprint may get disturbed and wrong minutiae points may arise.

In addition of these attacks, and by analyzing the fingerprints based identification system, we found that generally the enrolled fingerprint images are stored in a database along with the demographic text data of the individual and a facial image. The different data types are usually stored under three different sub categories in a database. The collection, storage and analysis of disparate

information introduces problems such as data mismatches and mishandling, high cost of storage, a longer time for retrieval, and unauthorized tampering of the files in the database (Noore et al., 2007). This leads to the decrease of the biometric system credibility (Figure 2). Ensuring the security and the integrity of biometric data has become a critical issue.

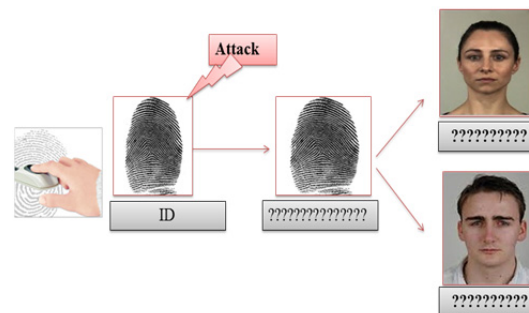


Figure 2: The attack after enrolment in AFIS system.

In order to solve this problem, this paper proposes an algorithm that combines a digital watermarking technique and an Arnold scrambling process. The digital watermarking approach is used to embed the iconic digital information (watermark) where in our case; it's composed of ID image and gray scale face image into the corresponding enrolled digital fingerprint of the person. Embedding the facial and ID data into the individuals fingerprint image eliminates data mismatch, reduces the high cost of storage, speeds the retrieval of related data and detects tampering. It is important to ensure that the embedded ID and face watermarks do not alter the functional integrity of the fingerprint and its ability to detect possible matches.

The unique robustness and security character of the watermark can ensure the integrity and reliability of the fingerprint data after information exchange process. So it can identify the authenticity of the contents, as well as content protection.

The proposed watermarking method is based on Shih approach (Shih and al., 2011), where he proposed a semi fragile spatial watermarking based on Local Binary Pattern operator (LBP) to embed a binary watermark. The operator takes a local neighborhood around each pixel, thresholds the pixels of the neighborhood at the value of the central pixel and uses the resulting binary-valued image patch as a local image descriptor.

In the proposed algorithm, the embedding process is performed on two levels. In the first level the binary ID image is inserted while the gray scale face image is embedded in the second level. To

improve the security of the embedding; the proposed technique employs the Arnold scrambling to preprocess on the watermark images, such that the watermarked fingerprint image has security under cryptography sense, for double protection.

2 THE PROPOSED METHOD

2.1 Arnold Scrambling Transform (AST)

Scrambling transformation as a means of encrypted technology (yothish et al., 2012) is applied as preprocess stage of the watermarking, after scrambling transformation, one meaningful watermarking will become a meaningless, chaotic image. If the scrambling algorithm and keys are not known, the attacker cannot recover it even if he gets the watermark from the embedded watermarking. Thus the Scrambling transformation plays a role of secondary encryption. Additionally, after scrambling transformation, it will upset the relationship between the space locations of pixels and make it evenly distributed in all space of the carrier image. This will improve the robustness of the algorithm. Two-dimensional Arnold scrambling transformation is defined as follows:

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \bmod N \quad (1)$$

wherein, X and Y are the pixel coordinates of the original space; X' , Y' are the corresponding pixel coordinates after iterative computation scrambling. The parameter N represents the size of the rectangular image, also referred to as a step number.

To restore the original initial watermark, the corresponding inverse transform formula is applied, it is given by:

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \bmod N \quad (2)$$

Arnold transformation is cyclical. If the cycle and the number of iterations are not known, the watermark is not restored. Therefore, cycle and iterations can exist as a private key.

2.2 Embedding Process

2.2.1 Fingerprint Pre-Processing

This task is performed by removing the noise using region based segmentation method, which presumes that pixels in the same regions are similar in such brightness and texture. After that the Region of Interest (ROI) is extracted and cropped from the denoising image. In proposed system, the fingerprint center point is automatically detected using the method described in (Julasayvake and Choomchuay, 2010) for the cropping region. Depending on this center point, the image of size $N \times N$ is cropped and used for watermarking process.

2.2.2 Embedding Process in One Level

The embedding process is applied in the spatial domain by using the original LBP operator and Boolean function operations defined in (Shih and al., 2011). The insertion is performed by adjusting one or more of the pixels in the neighborhood to make the Boolean function results consistent with the bits of the watermark. In our scheme, the watermark is composed of ID image and grayscale face image. The schematic diagram of the proposed embedding process is given in figure 3.

Step 1: The original fingerprint image $I(i,j)$ is subdivided in G non-overlapping blocks of 3×3 , to which the LBP operator (Ahonen et al., 2006) is applied to calculate the magnitude matrix (M_p) and the matrix $\text{sign}(S_p)$. The matrix M_i is constructed by calculating the absolute values of the difference between the gray level of the center pixel g_c and its 8 neighborhoods g_i as follows:

$$M_p = \{ M_i / M_i = |g_i - g_c|, i = 0, \dots, 7 \} \quad (3)$$

The matrix S_p is obtained by applying the operator LBP of the matrix G , it is given by:

$$S_p = \{ S_i / S_i = \text{sgn}(g_i - g_c), i = 0, \dots, 7 \} \quad (4)$$

where sgn refers to the sign function defined as:

$$f(x) = \begin{cases} 1, & x \geq 0 \\ 0, & \text{others} \end{cases} \quad (5)$$

Step 2: Calculating the Boolean function $f(S_p)$ by applying the XOR operator (\oplus) on the binary sign vector S_p as follows:

$$f(S_p) = S_0 \oplus S_1 \oplus \dots \oplus S_7 \quad (6)$$

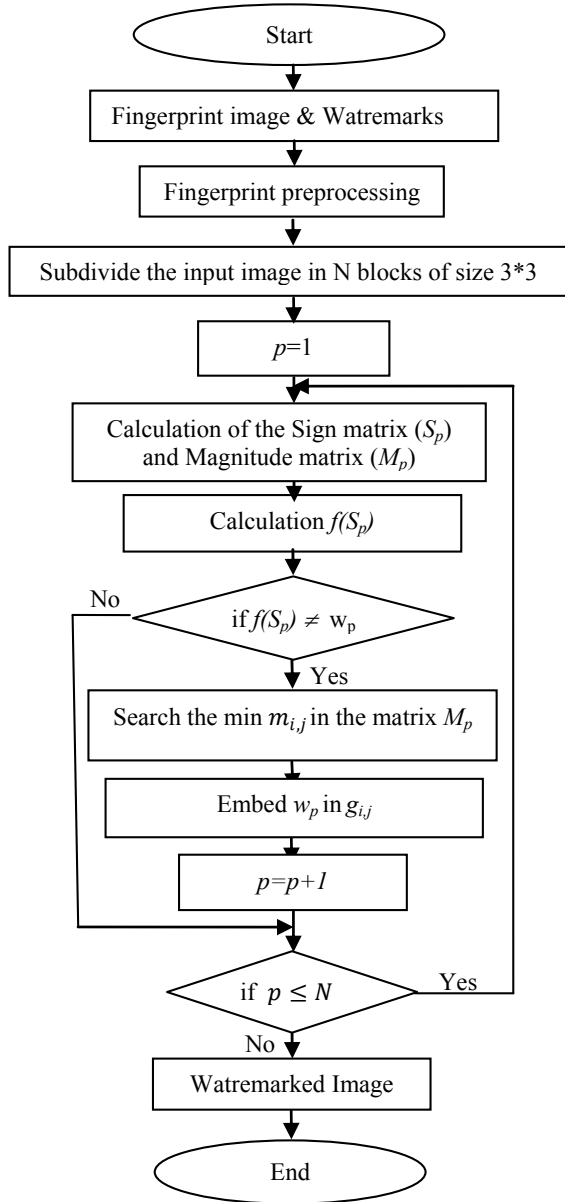


Figure 3: Schematic diagram of proposed embedding process.

Step 3: performs the embedding operation: to embed one bit of the watermark, we search the embedding location by comparing the value of the function $f(S_p)$ with the bit value w_k of the watermark. If they are different, we search the location $I(i, j)$ of the minimum value $m_{i,j}$ in the matrix M_p and, we modify the pixel corresponding to the similar position in the matrix G_p . Otherwise, we do nothing to the pixels in the neighborhood. The insertion operation is as follows:

if $(w_k \neq f(S_p))$ then

$$\begin{cases} \text{select } m_{i,j} = \min(M_p) \\ \text{if } (S_{i,j} = 1) \text{ then} \\ \quad g'_{i,j} = g_{i,j} + [-\beta g_{i,j} + m_{i,j} * (\beta - 1)] * \gamma_{i,j}; \\ \text{else} \\ \quad g'_{i,j} = g_{i,j} + [\beta g_{i,j} + m_{i,j} * (\beta + 1)] * \gamma_{i,j} \end{cases}$$

The parameter β represents the strength factor. γ takes the value 0 if the pixel (i, j) under consideration belongs to a fingerprint feature region like delta or core areas (singular points); it has value 1 otherwise.

To achieve higher embedding payload and better robustness, the embedding process is extended to double level. By this, we can insert not only the ID image of the person, but also other information such as the image of his face.

2.2.3 Embedding Process in Double Level

To perform the embedding in double level, the neighborhood S_p calculated in aforementioned embedding operation is divided in two parts even and odd neighbors, denoted by (S_e) and (S_o) respectively (Figure 4). After that, the functions $f(S_e)$ and $f(S_o)$ are computed and according to their values, two bits of the watermark are hidden such that each part hides one bit of the watermark. The embedding is done conforming to insertion process given above. In this way, the watermarking capacity is doubled.

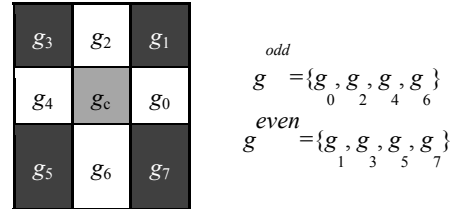


Figure 4: Partition of the matrix S_p in two sets even(S_e) and odd (S_o).

2.3 Watermark Extraction Process

The detection is performed in a blind manner which means that the original fingerprint image is not needed at the extraction. The watermark bits W_k are extracted from each part (odd and even) within a block after having calculated the matrix $f(S_e)$ and $f(S_o)$. According to their values, extracted bits are determined as follows:

$$w'_k = \begin{cases} f(S_e) & \text{if block part is even} \\ f(S_o) & \text{else} \end{cases} \quad (7)$$

3 EXPERIMENTS AND RESULTS

To gauge the performance of the proposed scheme, we carried out the simulation on fingerprint images of size (248*292). The watermark is composed of a binary ID image of size 240x22 and grayscale face image of size 35x35. This conducts to the embedded watermark data of (16092 bits).

The imperceptibility property determines how much the watermarked fingerprint image differs from the original fingerprint image; in other words, how much the embedding process distorts the host image. In this paper, the conventional image quality metric Peak to Signal-to-Noise Ratio (PSNR) is used as the criteria of imperceptibility. It is computed as follows:

$$PSNR(dB) = 10 \cdot \log \frac{255^2}{MSE} \quad (8)$$

with

$$MSE = \frac{\sum_{x=1}^m \sum_{y=1}^n (f(x, y) - f'(x, y))^2}{n * m} \quad (9)$$

where $f(x, y)$ and $f'(x, y)$ represent the pixel values of the original host fingerprint image and the watermarked image respectively. The parameters x , y specify row and column size of images respectively.

The extraction performance of watermarking is measured by the Error Bit Rate (EBR) or the error probability. The EBR is the number of extracted bits that have been altered due to noise, interference and distortion, divided by the total number of embedded bits. EBR is a dimensionless performance measure, often expressed as a percentage number (Xinhong, et al., 2012). It is given by:

$$EBR = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} (w_k[i, j] \oplus w'_k[i, j])}{n * m} \quad (10)$$

where $w_k[i, j]$, and $w'_k[i, j]$ denote the original watermark and the extracted one of $(n*m)$ size respectively.

As it can be seen from figure 5, the watermarked fingerprint images is decoded with 100 % decoding accuracy; also the watermarking does not change the fingerprint features of the original images as well the visual quality. This results in the PSNR equal to 36 dB.

In addition to imperceptibility and capacity criteria, the reliability of the watermarking approach correlates also with the robustness against the attacks. The main requirement of robustness is to resist different kinds of distortions introduced by common processing or malicious attacks while satisfying the imperceptibility criteria. Table 1 shows the robustness of the proposed method against some image-processing manipulations such as luminance manipulation, contrast enhancement, additive noise and JPEG compression.

Figure 6 shows the EBR curves after applying above mentioned manipulations using the two modes of insertion: simple embedding in which one bit of the watermark is embedded within the block of size 3x3 and double level of embedding where the block is partitioned in two parts even an odd. We notice that in double-level watermarking process the robustness against manipulations is better than in the simple embedding one despite the payload is two times larger.

The proposed scheme provides excellent results in term of the payload compared to the results obtained in (Jain and Uludag, 2003) and (Pravin et al., 2011) while keeping the subjective visual quality unchanged.

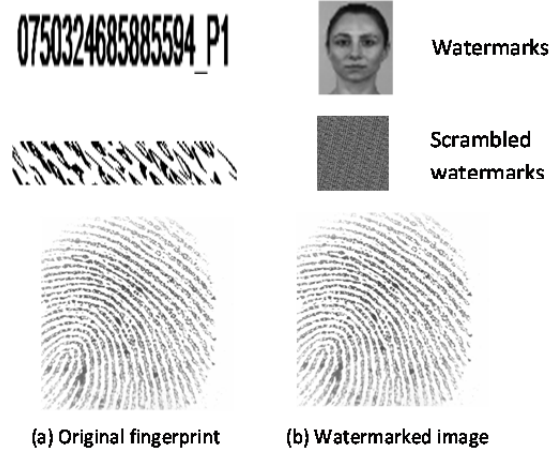





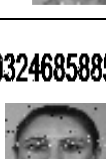

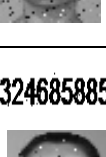




Figure 5: Subjective visual quality: (a) Original fingerprint image, (b), watermarked fingerprint image.

In term of protecting the biometric features of fingerprint image, in our scheme, we propose to protect the fingerprint feature region like delta or core areas by masking their pixels. The pixel takes the value 0 if the pixel under consideration belongs to a fingerprint feature otherwise it takes 1. Contrary to (Pravin et al., 2011) where the authors did not discuss how the biometric features are protected.

Table 1: Extracted watermarks resulting after some applying spatial attacks.

Attacked watermarked image	Extracted Watermarks	EBR (%)
 Cropping		7.85
		2.70
 Additive noise		1.69
		1.77
 Luminance manipulation		0.46
		0.8
 Contrast enhancement		0.2
		0.5
 JPEG Compression with quality 100		5.5
		4.32

4 CONCLUSIONS

In this paper, a local adaptive watermarking method based on LBP operator is presented to provide data integrity and authenticity of the fingerprint images content. The embedding consists of hiding the identifier (ID) image and the face image in the corresponding fingerprint image after being enrolled by the AFIS system. This process eliminates data mismatch, reduces the high cost of storage, speeds the retrieval of related data and detects tampering. The results show that the criterion for imperceptibility is achieved; the fingerprint images

are watermarked without changing the features associated with them. The robustness against some spatial attacks is provided. However the proposed scheme is not prove to be robust to WSQ (Wavelet Scalar Quantization) compression.

As fingerprint images are often compressed using an open wavelet-based image compression (WSQ) developed by the FBI, we are working to improve the robustness against WSQ by introducing the error code coding (ECC) before the embedding process and doing the embedding in frequency domain.

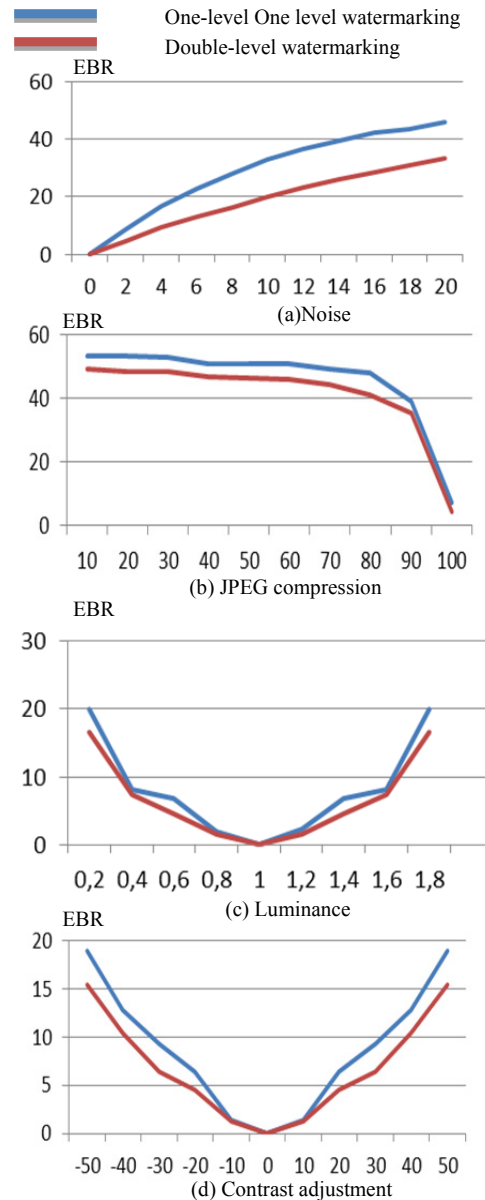


Figure 6: Resulting EBR against the spatial attacks.

REFERENCES

- Ahonen, T., Hadid, A., Pietikäinen, M., 2006. Face description with local binary patterns: Application to face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 2037-2041.
- Jain, A. K., Uludag, U., 2003. Hiding biometric data. *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 25, no. 11, pp. 1494–1498.
- Julasayvake, A., Choomchuay, S., 2010. An algorithm for fingerprint core point detection. *International Journal of Computer Applications*, vol. 2, n°. 8, pp. 0779 – 4244.
- Mathivadhani, D., Meena, C., 2010. A comparative A Comparative Study on Fingerprint Protection Using Watermarking Techniques. *Global Journal of Computer Science and Technology*, vol. 9, Issue 5, pp. 98-102.
- Noore, A., Singh, R. Vatsa, M. and Houck, Max M., 2007. Enhancing Security of Fingerprints through Contextual Biometric Watermarking. *Forensic Science International*, Issue 169, no. 2, pp. 188-194.
- Uludag, U., Jain, K., 2004. Attacks on Biometric Systems: A Case Study in Fingerprints. In: *Proc. SPIE-EI, Security, Seganography and Watermarking of Multimedia Contents VI*.
- Wenyin, Z., Shih, F.Y., Faugeras, 2011. Semi-fragile spatial watermarking based on local binary pattern operators. Elsevier, 3904–3912.
- Xinhong, Z. Fan, Z., Li, D and Li, C., 2012. An Analysis of Relationship of Watermarking Decoding Error Bit Rate and Payload Capacity. *Journal of Computational Information Systems* vol. 8, n°. 20, pp. 8431–8438 Available at <http://www.Jofcis.com>
- yothish. J., Prabhu, V., Kumar, S., 2012. A Robust Watermarking method based on Compressed Sensing and Arnold scrambling. *IEEE Machine Vision and Image Processing (MVIP)*, pp.105-108.