Visual cryptography applied to fingerprint features as a solution for pre-alignment

Julien Bringer
Morpho

Hervé Chabanne
Morpho, Télécom ParisTech

Abstract: Visual cryptography enables to derive from an image two shares that give separately no information on the original image while leading back to the image by superimposition of the shares. In this work, we apply this technique to fingerprint features for enabling a blind alignment of a reference and a fresh image. The idea is to use an encrypted share derived from the reference data as a kind of reference for pre-alignment of the fresh data on it. Following the principle of visual cryptography, it also ensures a storage protection when data are stored in separate locations.

1 Introduction

When quantizing biometric data (from images or templates), one important issue is the difference of alignment between the capture at enrollment and the verification's one. This is even critical for modality such as fingerprints where there is almost none reliable information that can be used to pre-align the image at the encoding step. Several methods of fingerprints quantization (based on images or on minutiae templates) are suggested in state-of-the-art, as for instance [JPHP99, TAK+05]. Unfortunately, most of them gets poor performances in misalignment situation. They then need either exhaustive search on the orientation/translation or a preliminary registration step before comparison.

Related to those works on the protection of biometric data, we here present a solution for a user to align two fingerprint "visually" by having only a portion of the reference image. This solution aims at allowing to pre-align two fingerprints without using of techniques directly bound to the biometrics. Note that although the main motivation is fingerprint, this can be applied to other modality that are captured at some step as an image.

Our technique can be applied as a visual help to a user who can see on a dedicated screen the effect of the superimposition of one stored share with his freshly capture finger and react accordingly to improve the quality of this image. We can also think to an automatic treatment of the image.

Within the context of protection of biometric data, for instance for secure sketches technique where the noise introduced from a biometric measure to the other one is corrected by means of correcting codes of errors, the alignment of the data is often critical.

In particular, this problem arises in the case of fingerprints because there is no natural binary vector representation directly usable – contrary to the case of the iris where the format of iriscodes is compatible as it is. The main difficulty in the alignment is due to

the fact that during verification check, we do not have, contrary to the case of classical matching, a reference fingerprint "in clear" such that the fresh capture can be aligned with. These problems of alignment between several measures of the same fingerprint are due, in particular, to the positioning of the finger (global translations / rotations) and to the exercised pressure (local distortion). This alignment issue for protection techniques is underlined in [TAK+05, UPJ05] without being effectively resolved even in the recent advances.

For example, on the 2 images of Figure 1 which result obviously from the same fingerprint, we can notice that the gap is very important (important translation, low rotation and distortion), while the score of matching will be relatively good. If we use these images without any pre-alignment in most quantization algorithms for secure sketches, it will not then be possible to correct the noise, because the noise introduced by the lack of alignment is very high: it is thus useful to be capable of pre-aligning these 2 images to process them correctly.

(a) Reference image (b) Fresh image

Figure 1: Example of difference between reference and verification images

A first idea could be to store a part of the left image as the reference (for example a small portion of the center of the image or several sub-images) to pre-align globally the right image above. But this technique does not allow to pre-align finely the points of the image situated outside the reference portion. Moreover, this forces to store some information in clear. Other techniques exist, based for instance on reference points (core, delta, UCX, ... [SOISO05]) or more complete description (e.g. high curvature points as in [NRV10]), but they are either non universal, non stable enough or directly leak some information on the global shape.

2 Visual Cryptography

The visual cryptography notion, as introduced by [NS94], is to ensure the protection in confidentiality of an image while allowing a simple and visual reconstruction. The general principle is to split an image I in m pieces $(s_1, \ldots, s_m)$ so that the knowledge of k pieces among these m pieces (with $k < m$) gives no information on I. The knowledge of m pieces allows to build a new version of the image I (according to the employed techniques,

the resultant image will be a version of I that is more or less degraded). It thus corresponds to a sharing of secrets with visual reconstruction.

An example of visual cryptographic scheme, in the case of the sharing of an image in black and white in 2 pieces, is the following one. Every pixel of the original image I is subdivided into a sub-pixel of 4 pixels in the shares s_1 and s_2 where every sub-pixel has one of the forms given by Figure 2. A white pixel is shared in 2 identical forms and a black

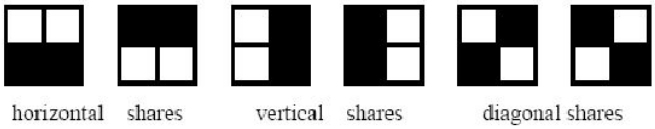
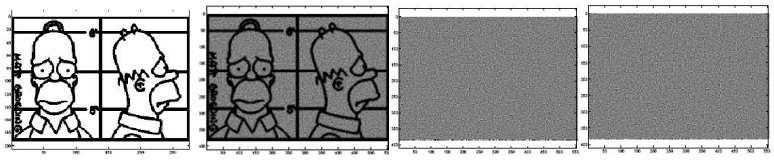


Figure 2: Sharing of a pixel in 2 shares (sub-blocks of 4 pixels)

pixel is shared in two complementary forms. Every couple (f_1, f_2) of forms obtained is separated to store the first constituent f_1 in the first share s_1 and second constituent f_2 in s_2. In both cases (white pixel and black pixel), the forms to be used are randomly chosen. This thus implies that a share alone leaks no information about the original image. Finally, when 2 shares are superimposed, we obtain by transparency an image representing the original image with grey sub-pixels (blocks of 2 white and 2 black pixels represent a white pixel in the original image) and of black sub-pixels (for the black pixels of the original image). Figure 3 gives an example of visual cryptography applied to a whole image.

The operation of transparency corresponds in fact to a OR following the rules: white OR white = white, black OR white = black, black OR black = black and white OR black = black.



(a) Original image (b) The reconstructed image (c) The two shares

Figure 3: Example of visual reconstruction by transparency of 2 superimposed shares

3 Visual cryptography for fingerprint alignment

Given a reference biometric data b_{ref} at enrollment, we split it in two share (s_1, s_2) according to a principle of sharing of secrets, as explained in Section 2, to obtain a safe splitting (no single share will reveal information on b_{ref}). During the verification check,

the fresh biometric data b_{fresh} is divided in two shares (s'_1, s'_2) so that we will be able to combine properly s_1 and s'_2 to realign b_{fresh} on b_{ref} without revealing completely b_{ref}. More exactly, the principle is the following one.

Enrollment:

- Capture a reference biometric data b_{ref};
- establish a splitting strategy Γ randomly that consists of a vector of couples that can be used to represent a white pixel and a black pixel (in fact for each position in the image, a couple of valid representation as in Figure 2 of a white pixel and a black pixel is chosen randomly to construct Γ) ;
- split the image in two shares s_1 and s_2 following the splitting method Γ;
- store s_1 in one database DB_1, and Γ in a second one DB_2.

Γ is in fact a vector of same size that the image; at position i, $\Gamma[i]$ is a couple (W, B) that corresponds to the representatives chosen respectively for a white pixel and a black pixel. We have $W = (W_1, W_2)$ and $B = (B_1, B_2)$ with W_j (resp. B_j) corresponds to the block (4 sub-pixels in the case of Figure 2) to be inserted in the share s_j if the original image has a white pixel (resp. a black pixel) at position i. The method Γ is chosen randomly in particular so that from s_1 or s_2 it is not possible to find b_{ref}, i.e. Γ distributes well the information in s_1 and s_2.

Verification check:

- Capture a fresh biometric data b_{fresh};
- retrieve the method Γ of the claimed identity in the second database DB_2;
- split b_{fresh} in two shares s'_1 and s'_2 according to this method;
- retrieve the share s_1 of the claimed identity in the first database DB_1;
- combine s_1 and s'_2 to determine the geometrical transformation that leads to the image of best quality.

The phase of verification check requires a mean of control, automatic or manual, of the quality of an image: we can use for example the neatness of the image. Once this geometrical transformation determined (for instance by semi-exhaustive search, starting with a large step and fine-tuning the step of the search progressively), we apply it on b_{fresh} before passing in a next stage (e.g. secure comparison, key extraction, ...).

The specificity of this algorithm within the context of biometrics compared to classical application of visual cryptography techniques is that the reconstruction is made from an original share s_1 and a fresh share s'_2 that is not s_2 but a noisy version of the original share s_2.

Remark 1 *Note that, as our main goal is to provide an assistance for alignment, we can even imagine to use a visual feedback on a sensor where a user will be able to modify the position and pressure of the finger to improve the neatness of the obtained result.*

Remark 2 *From a practical point of view, we can also make the alignment in a symmetrical way by using the two original shares. Indeed, if we have the shares s'_1 and s'_2 of the fresh capture, we can try to combine simultaneously s_1 with s'_2 and s'_1 with s_2 to refine the determination of the optimal alignment. Note that in that case, a strict separation of the storage location for the shares is needed if any confidentiality requirement.*

4 Examples

For two different captures (here fingerprint images) coming from the same finger, we first convert the images in black and white and applied the algorithms (for enrollment and verification check) described in Section 3. With the fingerprint images from Figure 1, we obtain the two shares s_1, s_2 from the image of Figure 1a (where only s_1 will be kept) and we obtain the share s'_2 from the image of Figure 1b. We remark that none of these shares alone allows to guess the original images.

We then combine s_1 and s'_2 to search for the best translation according to the quality of the reconstructed image: this is illustrated by Figure 4.

(a) Image reconstituted without translation

(b) With an intermediate translation

(c) With the best translation

Figure 4: Different translations applied for reconstruction of the superimposed image from s_1 and s'_2

To check the efficiency of the method, we can use a classic matcher to find the best translation between the sets of minutiae extracted from those images. From Figure 4, the translation obtained for the clearest result fits well with those one returned by a matcher.

Remark 3 *The noise appearing at the external boundaries of the image is an effect of the translation, it corresponds to areas outside the second fingerprint image.*

Now, we try to combine the share s_1 with a share coming from a non matching fingerprint,

we then obtain less clear images, whatever the translation is – cf. Figure 5. Without translation fingerprints do not correspond at all, and even with the ideal translation calculated by a minutiae matcher, there are still areas of important noise.

(a) Non-matching fingerprint with fingerprint from Figure 1a

(b) Image reconstituted without translation

(c) With the best translation

Figure 5: Different translations applied for reconstruction of the superimposed image from the shares of two non-matching fingerprint images

References

[ISO05] ISO/IEC 19794-2:2005. Information Technology, Biometric Data Interchange Formats, Part 2: Finger Minutiae Data. Technical report, ISO/IEC, 2005.

[JPHP99] Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharath Pankanti. FingerCode: A Filterbank for Fingerprint Representation and Matching. In *CVPR*, pages 2187–. IEEE Computer Society, 1999.

[KJR05] Takeo Kanade, Anil K. Jain, and Nalini K. Ratha, editors. *Audio- and Video-Based Biometric Person Authentication, 5th International Conference, AVBPA 2005, Hilton Rye Town, NY, USA, July 20-22, 2005, Proceedings*, volume 3546 of *Lecture Notes in Computer Science*. Springer, 2005.

[NRV10] Abhishek Nagar, Shantanu Rane, and Anthony Vetro. Alignment and bit extraction for secure fingerprint biometrics. In Nasir D. Memon, Jana Dittmann, Adnan M. Alattar, and Edward J. Delp, editors, *Media Forensics and Security*, volume 7541 of *SPIE Proceedings*, page 75410. SPIE, 2010.

[NS94] Moni Naor and Adi Shamir. Visual Cryptography. In *EUROCRYPT*, pages 1–12, 1994.

[TAK+05] Pim Tuyls, Anton H. M. Akkermans, Tom A. M. Kevenaar, Geert Jan Schrijen, Asker M. Bazen, and Raymond N. J. Veldhuis. Practical Biometric Authentication with Template Protection. In Kanade et al. [KJR05], pages 436–446.

[UPJ05] Umut Uludag, Sharath Pankanti, and Anil K. Jain. Fuzzy Vault for Fingerprints. In Kanade et al. [KJR05], pages 310–319.