Multiple Watermarking Enhances Security of Fingerprint Images

Afzel Noore, Mayank Vatsa, Richa Singh, Keith Morris, and Max M. Houck

Identity cards, driver's license, and passports routinely require additional biometric information such as fingerprints and photographs to establish the identity of an individual. This information is stored in different databases along with the individual's demographic text data. The personal information must be protected to prevent tampering, deter identity theft, and possible misuse. Digital watermarking is a technique used for hiding information imperceptibly in an object to protect the integrity of data. A novel contextual digital watermarking for law enforcement application is presented. It securely embeds the demographic text data and the face image as watermarks in the fingerprint image of an individual.

Electronic capture of fingerprint images using live-scan systems is becoming prevalent. Demographic data such as, name, date of birth, and other information pertaining to an individual's identity is conveniently entered electronically using a keyboard. The text information, along with the digital fingerprint images are compressed and formatted according to the approved standards and either stored or transmitted electronically. The use for Automated Fingerprint Identification System (AFIS) for fingerprint matching has dramatically increased and continues to permeate from forensic applications in criminal investigation to non-forensic applications such as immigration control, national ID and driver's license, welfare disbursement, health care system, access control, and e-commerce.

When using a fingerprint or face for the purpose of identifying an individual, it is of paramount importance to ensure the integrity of digital evidence. Many tools and methods can easily alter and manipulate the attributes of digital objects to commit fraud or identity theft. Another important research issue that needs to be considered when using digital imaging technology is the chain of custody, especially when it is used as evidence in solving criminal cases. Latent fingerprints subjected to sequence of transformations for analysis must be documented such that it yields consistent results when the process is repeated. The goal of instilling high confidence and trust in the evidence collected and subsequent analysis should eliminate providing any opportunity for unauthorized persons to access, tamper, or substitute an image. If the integrity or trustworthiness of the fingerprint image is questionable, it may be liable to legal challenges.

Techniques such as encryption and digital watermarking are currently used for the purposes of authenticating the integrity of photographic images and for copyright protection. The process of

encrypting or embedding watermarks causes the original data image to change even though the minor changes are visually imperceptible. Several watermarking techniques for images have been proposed. These techniques are designed to ensure that they are robust to external attacks and the watermarked images are a replica of the original images with negligible degradation in quality. Similar techniques can also be applied in biometrics to enhance security and reliability of various applications.

Challenges in biometric watermarking

For applying watermarking techniques to biometric images, it is not sufficient to verify if the watermarked biometric image closely resembles the original image. It is important to ensure that various characteristics and features of the biometric image be preserved to accurately process and analyze correctly. For example, fingerprint classification can provide an important indexing mechanism in a fingerprint database. An accurate and consistent classification greatly reduces fingerprint matching time. Therefore, when assigning a fingerprint image to pre-defined category a watermarked fingerprint image should yield the same classification result as the original fingerprint image. Also, when comparing an unknown fingerprint of an individual with fingerprints in the database, the AFIS should produce the same result whether the fingerprint images stored in the database is watermarked or not. Furthermore, there is a need for fingerprint images to be electronically transmitted over a communication channel. This introduces some degradation in the fingerprint image. For example, images are compressed when transmitting over low bandwidth channel. During transmission, some noise in the transmission channel maybe introduced. However, these functions should not affect the matching performance of either the fingerprint image or the watermarked image. There are a number of other geometric and frequency attacks such as blurring, filtering, scaling, rotation, and cropping, which can degrade the quality or distort the features of a fingerprint image. The watermarking algorithm should be designed to be resilient to such attacks and also ensure that the identification accuracy is not affected.

Existing approaches

Limited studies have been undertaken to embed a face image of an individual as a watermark in the fingerprint of the same individual. Researchers have used spatial, frequency, or wavelet based techniques to embed a face image or selected face features in the fingerprint image. Fingerprint image is used as the base or cover image, and facial features such as eigen vectors are used as the watermark data. In a fingerprint image, the areas which contain minutiae are critical for matching. These regions are first identified and isolated to ensure the integrity of the fingerprint and accuracy of matching. Facial features are then embedded in non-critical regions of the fingerprint image. The watermarked fingerprint image contains the embedded facial features and is stored in the database for matching purposes.

Contextual biometrics watermarking

The research performed for the United States Department of Justice uses a novel multi-watermarking approach that embeds two distinct watermarks in a fingerprint image. Many applications pertaining to criminal justice, or driver's license or e-passport use one or more biometric traits of an individual and store them with the demographic data of an individual. For example, driver's license stores face and fingerprint of the user along with demographic data, e-passports also plan to include face and fingerprint of the individual along with demographic details. Currently, the face, fingerprint, and demographic

information are stored in three indexed databases. The proposed approach seamlessly integrates all three objects into a single image that can conveniently be stored in one database.

Watermarking embedding and extraction process

In this research, we developed an algorithm to embed both the face and the demographic data in a fingerprint image efficiently. The fingerprint image is first transformed into three-level wavelet transform and the features important for matching are identified. These features are the minutiae points which are located at the ridge ending or bifurcation. The edges in the wavelet domain can be used to identify these features. A key is generated that contains selected locations from the non-critical regions of a fingerprint. From an individual's face image, eigen vectors are generated. These eigen vectors and the demographic data are embedded into the wavelet transformed fingerprint image according to the key. The face and demographic information are embedded multiple times in different levels of the wavelet transform to make it resilient to external manipulations. This embedding also ensures that the fingerprint features required for matching are not affected. The watermark embedded wavelet coefficients are reconstructed to produce the watermarked fingerprint image. Figure 1 shows the fingerprint watermarking process. The watermarked fingerprint contains an individual's face image and demographic data and looks striking similar to the original fingerprint. The watermarked fingerprint image is then stored in the database. Such a technique reduces the database size, is compatible with existing AFIS for matching, and makes the demographic and the face objects invisible from tampering. This watermarked fingerprint image is used for matching purposes. If a match is found, the face image of the individual and related demographic data is easily extracted from the watermarked fingerprint for further cross validation or visual comparison.

To extract the face and demographic data from a watermarked fingerprint, the reverse process used during embedding is employed. The watermarked fingerprint image is transformed into wavelet domain and the watermark objects are extracted using the same key generated during embedding. The key can be stored in the database or it can be computed for every image depending on the image features. Figure 2 shows the watermark extraction process. The extracted facial features and the demographic data of an individual can be used for automatic matching. Or alternatively, a manual comparison can be made using the extracted demographic data and reconstructed face image.

Conclusion

Depending on the requirements of an application, the extracted watermarks can effectively validate the authenticity of an object embedded in a document or an individual's identity. In addition, since information is embedded in different levels of the wavelet transform it makes the approach robust and resilient to different frequency attacks. The approach can also detect tampering due to geometric manipulations and alterations. Instead of using multiple databases for storing fingerprints, face images, and demographic data, the watermarking approach stores only a single image, thereby saving memory while protecting the integrity of fingerprints. It detects if any character in the text is altered or if the face image features have been tampered. From an operational perspective, it enables law enforcement personnel to conveniently extract the personal information and face image of an individual from the watermarked fingerprint without the need to access disparate databases.

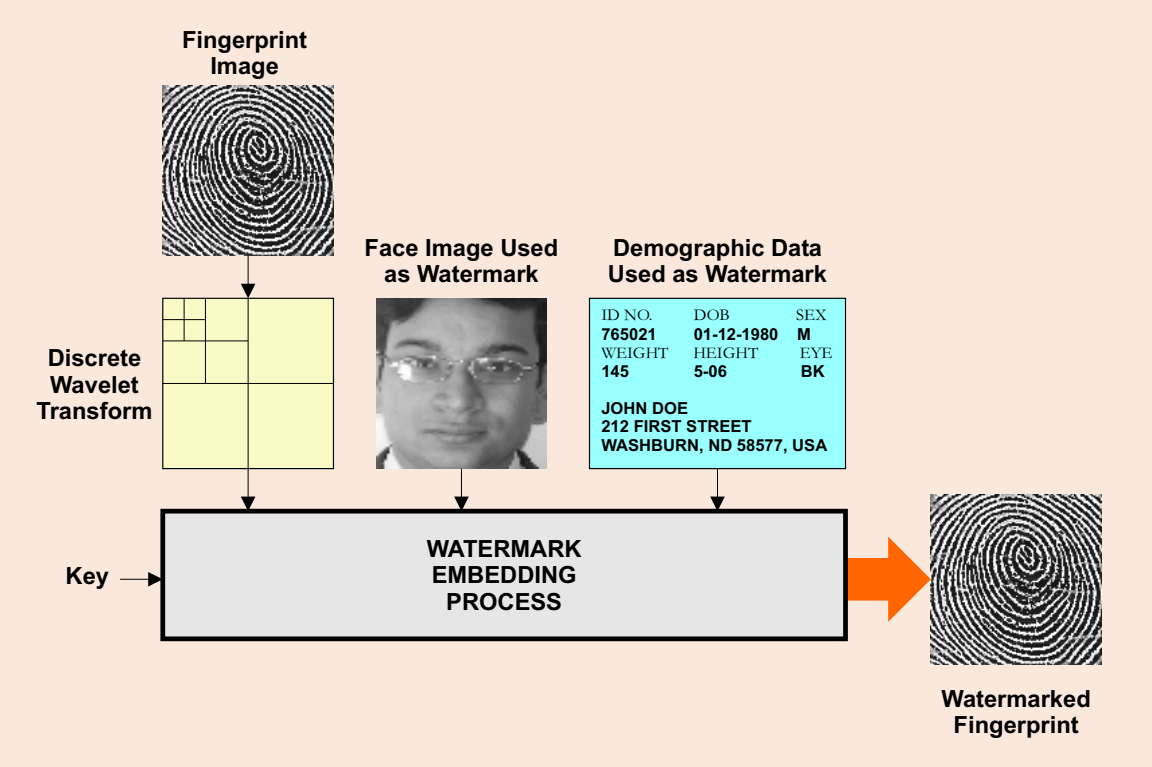

Figure 1: Embedding multiple watermarks in fingerprint image

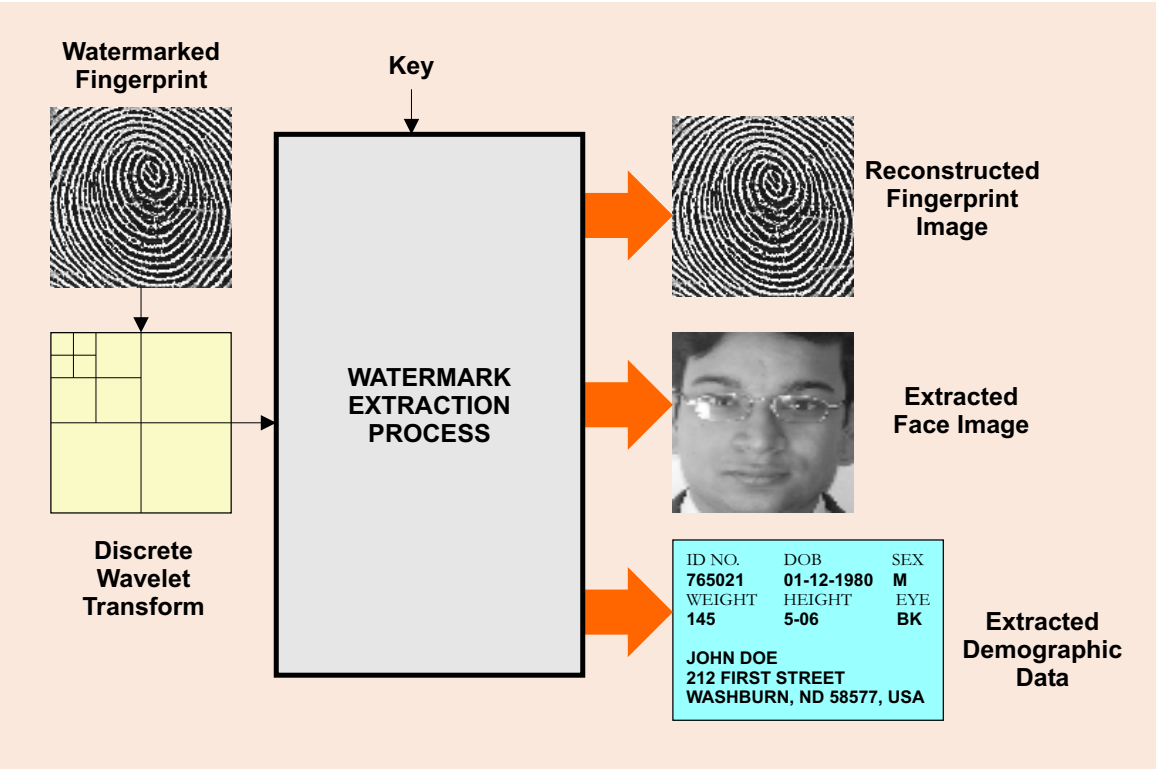

Figure 2: Extracting watermarks from watermarked fingerprint image