IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 11, November 2016

# A Novel Study on Multi-Tier Biometric Security using digital Watermarking

**Sheikh Imran[1], Shekhar Verma[2], Junaid Gillani[3], Suhail Nehvi[4]**

Student, M. Tech, ESSEAR, Ambala[1]

Assistant Professor, Dept. of EE, E-Max group of Institutions, Ambala[2]

Head, Department of Electronics and Communication, J&K Technical Education[3]

Lecturer, Govt. Polytechnic for Women, Srinagar[4]

**Abstract:** This paper presents multitier biometrics using watermarking algorithms with two levels of security for simultaneously verifying on individual and protecting the biometric template. The fingerprint as unique biometric templates is used as a watermark for digitally signing images linked to the watermark. The image can be used directly for verification and the watermark fingerprint data is used to cross authenticate the individual any attempt to tamper the image will consequently change the watermark embedded within it and create a discord between the embedded watermark and biometric data obtained on verification.

**Keywords:** Watermarking, Biometrics, Fingerprints, Authentication.

## 1. INTRODUCTION

Biometric data is data inherent to one's body, and almost always is unique to an individual. There are many forms of biometric identifiers. These include, but are not limited to: fingerprints, retinal scans, DNA, voice, gait, hand shape, signatures (not only the shape, but also the pressure used and the speed it takes to sign), and facial scans [1]. Unfortunately, some biometric identifiers, such as siblings' facial scans and identical twins' DNA are not unique.

In addition, some forms of biometric data do not work well in large groups, such as facial scans, palm shape scans, and a person's gait, but these data are easy to gather, and work very well for a small group. Biometric data's uniqueness makes it an effective form of identification, as the user does not need to remember a password, Personal Identification Number (PIN), or carry an identification card.

All the user needs to do is scan a fingerprint, retina, or use another unique identifier. However, just like any other identification system, there are security issues inherent to biometric identification. Not only are standard security issues such as insecure databases present, but the presence of a biometric scanner invites other forms of manipulation, such as mimicking a person's gait, or providing a copied fingerprint.

Furthermore, if someone were to gain access to a database of biometric identifiers, the intruder could potentially access a person's fingerprint, retinal scan, or other information, which a user would like to keep secret [2]. In addition to these issues, biometric identification carries risks which are unique to it.

In a traditional password or other authentication system, the user wants the information to be private. This privacy is what makes the authentication system work. Biometric information is not at all private.

People leave their fingerprints everywhere, a retinal match could be made with a high-resolution photo; and anyone who would like to mimic someone's gait simply needs to observe him or her for a period of time. Additionally, if someone gains access to a biometric identifier, that identifier is permanently compromised. If someone guesses our password, it is usually trivial to change that password. However if someone gains a copy of your finger print scan, we can only change this identifier nine more times, by switching fingers.

In the cases of retinal and palm scans, we can change this information once, and in the cases of DNA and facial scans, once someone obtains our identifier, we need to change the authentication system in order to keep them out. Similarly, if someone guesses a password that you use for multiple systems, it is usually trivial to change it across all of the systems. However, if someone obtains your biometric identifier, they can use it to access anything which you use that identifier for. The manner in which biometric data is stored is also relevant. Some forms of biometric data, such as a fingerprint, can change based on how much oil the skin has, or cuts on the finger. Because of this, precise matching is often impossible, so the traditional method of hashing (reducing a large segment of data into a smaller one which is based on the larger segment) does not work, as the differences can cause a different hash to be developed

DOI 10.17148/IJIREEICE.2016.41121

## II. ISSUES IN SECURING BIOMETRIC INFORMATION

There are several things by which we can secure biometric information:-

PHYSICAL SECURITY

One method of protecting a scanner is to increase the physical security present. This can include adding a person or camera watching the scanner, or requiring a password to access the scanner. This however would defeat the purpose of biometric identification, and is not recommended.

Because these methods do not involve the biometric system itself, they will not be further discussed in this paper. However, it is oftentimes trivial to get around these methods, so while the use of them can help, a determined attacker should nothave any difficulty bypassing them.

**SECURING YOUR SCANNER:**

One of the simplest methods of preventing a physical attack is to add complexity to your scanner. In order to protect against false fingerprints or retinal scans, a heat sensor could be used to ensure that a real finger or eyeball is being used [3]. A signature scanner could include a pressure pad to ensure that a user is not trying to trace a copy of someone's signature.

SECURELY MATCHING FINGERPRINTS

Shenlin Yang and Ingrid M. Verbauwhede of UCLA proposed a method of securely matching fingerprints [4]. Commonly used methods include image-based matching, graph-based matching and minutiae-based matching. Minutiae-based matching compares the differences in the details of the Fingerprint instead of the fingerprints themselves for a match. Such details include the types of minutiae present, and their distance from each other [5].

Fingerprint minutiae are minor details in the fingerprint which set it apart from other Fingerprints. Major types of minutiae include ridge endings, ridge bifurcations, ridge enclosures, short ridges, islands, spurs, crossovers, deltas, and cores [6]. Image-based matching uses the entire gray scale finger-print as a template to match against other fingerprints.

This method is very inconsistent, as it is difficult to account for minor variation. Graph-based matching represents the minutiae in the fingerprint in the form of graphs. However, this method has a very high computational complexity, which limits its practical use.

Because a minutiae-based matching system uses more discriminating and reliable features, and provides higher processing speed and a much lower template size of biometric information, Yang and Verbauwhede decided to base their system on minutiae matching.

The authentication algorithm works by comparing a minutia's neighbors to the neighbors of the corresponding minutia in the database; the neighbors of the lower circled island would be the circled bifurcation and enclosure. As stated earlier, the security of the biometric data itself is important, not only the scanner.

To address this concern, some biometric systems try to move the signal processing and matching engines from the server to the embedded device (in this case, the biometric scanner). In this type of system, the biometric data is processed and matched within the scanner itself, and the result of the processing and matching is sent to the server, instead of the full fingerprint.

This approach avoids many attacks on the communication between the scanner and the server, and on the server itself. Unfortunately, it is relatively simple to compromise the biometric templates which are stored in the scanner. As a result, the template is often encrypted. When a request comes in, the encryption key is used to decode the template, which is then used to process the input. However, this key is able to be extracted by analysis of external effects such as timing, electromagnetic radiation, and power consumption.

This type of attack is called a Side Channel Attack (SCA), and the most common form of SCAs is a Differential Power Analysis (DPA). A DPA is an attack which monitors the power usage of the device, and can tell a match by the different power consumptions. SCAs are most effective against a portable device, as there is often not enough room to add excess processing to be used as noise to trick the attacker.

## III. APPLYING DIGITAL WATERMARKING FOR SECURING BIOMETRIC INFORMATION:

We propose a multi–tier biometric security system. This is different from multimodal system. A multimodal biometric identification system is a system which uses multiple forms of biometric identification in order to provide additional security. Increasing the number of identifiers used makes it more difficult for an attacker to gain access. Not only would the attacker need to acquire additional information for a physical attack, but the systems can combine the different identifiers in clever ways to make the data more complex, thus harder to imitate.

USING PALM AND KNUCKLE-PRINT

Sun et al. proposed a system which uses both palm-prints and knuckle-prints [7]. Sun et al. suggest using the palm-print as the main identifier, but also discretely taking a knuckle-print scan, which would be used not only as another identifier, but it would also be used to provide a watermark for the palm-print. A watermark is data hidden in an image in order to ensure legitimacy. A common example is the red and blue threads in American currency.

DOI 10.17148/IJIREEICE.2016.41121

The system begins by scanning the knuckle-print, and using that scan to extract feature data. This feature data is then used to create a watermark, which is embedded into the palm-print image. During the authentication phase, the watermark is extracted from the palm-print, providing the original knuckle-print feature data. This data, in addition to the palm-print, is scanned against the database to validate whether the person is an authorized user. In addition to the watermark, the knuckle print provides a layer of physical security.

The knuckle-print scanner is built into the palm-print scanner, so an unauthorized user may not notice that they need to provide both the knuckle-print and the palm-print. This practice is often referred to as security through obscurity and is usually discouraged, since a security system should not rely on an attacker not knowing its details, only on his inability to forge a required identification. However, the benefits provided by watermarking still makes the second identifier useful, since forging two identifiers is more difficult than forging one.

## IV. USE OF PROPOSED MULTI-TIER SYSTEM

Multimodal systems are cumbersome and in most practical application use of photograph or a digital image is essential. By contrast in a multi-tier system, a biometric data is used to digitally sign an image to secure both the image and at the same time keeping the biometric data secure.

In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Ideal properties of a digital watermark have been stated in many include

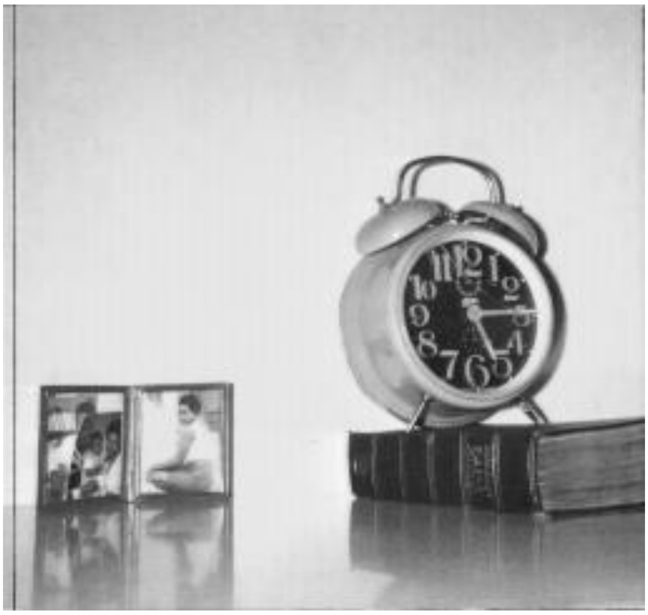
i) A digital watermark should be perceptually invisible to prevent obstruction of the original image.
ii) A digital watermark should be statistically invisible **so** that it cannot be detected or erased.
iii) Watermark extraction should be fairly simple; otherwise the detection process requires too much time computation.
iv) Watermark detection should be accurate. False positives, the detection of a non-marked image ,and false negatives, non-detection of a marked image, should be few.
v) Watermarks should be robust to filtering, additive noise, compression and other forms of image manipulation.
vi) The watermark should be able to determine the true owner of the image.

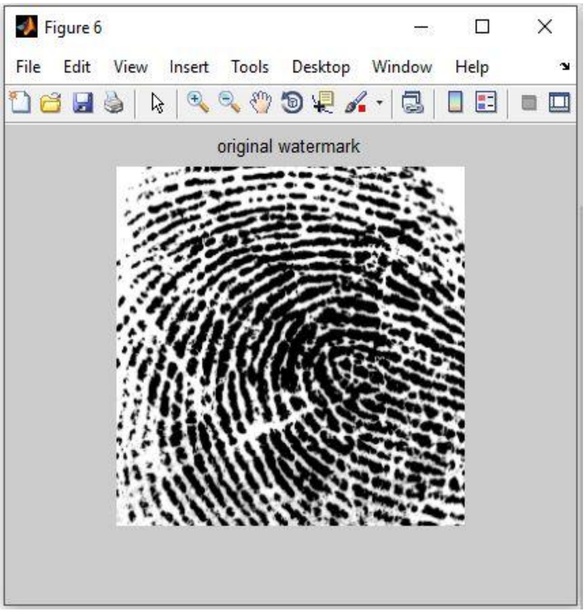
Two additional factors relating to capacity and speed are of major concern in securing the biometrics template in the proposed multitier biometric system. The watermarking system must allow for a sufficient amount of information to be embedded into the image.

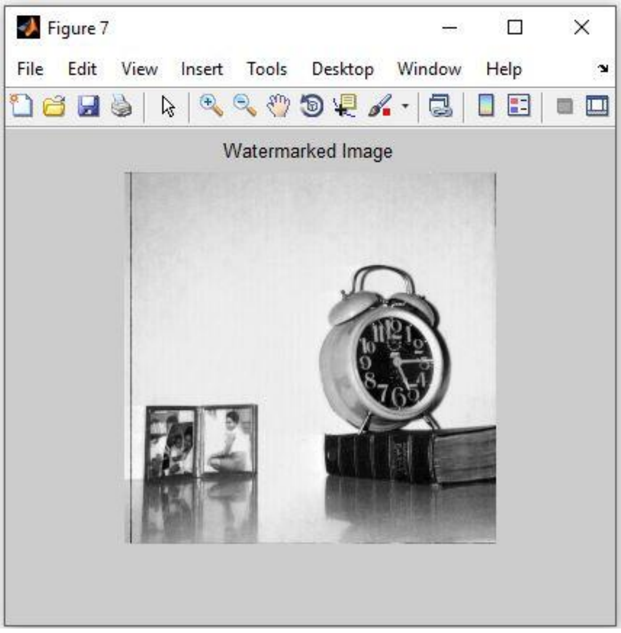
Furthermore, in watermarking systems designed for embedded applications, watermark detection or embedding should not be overly computationally intensive so as to preclude its use in biometric systems.

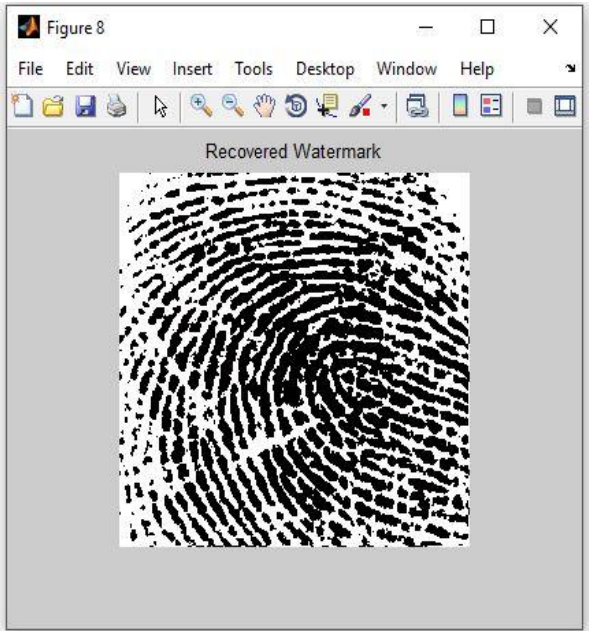
## V. RESULTS

An image database of different images available at USC-SIPI database was used to test the proposed multi-tier biometric system. This database consists of different images without any copyright protection. The biometric fingerprints were provided by volunteers to the authors. The watermark embedding and retrieval was successfully carried using LSB and DCT methods.









## REFERENCES

1. Schneier, B. Inside risks: the uses and abuses of biometrics. Commun. ACM 42 (August 1999.
2. Wikipedia. Biometrics wikipediahttp://en.wikipedia.org/w/index. php?title Biometrics, 2011
3. Kim, W., and Lee, H. Multimodal biometric image watermarking using two-stage integrity verification.Signal Processing 89, 2 (2009), 2385- 2399.
4. Yang, S., and Verbauwhede, I. M. A secure fingerprint matching technique. In Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications (New York, NY, USA, 2003), WBMA'03, ACM, pp. 89{94.
5. Liu, L., Yang, J., Chaozhe, Z., and Jiang, T. Information theory based fingerprint matching. IEEE Transactions on Pattern Analysis and Machine Intelligence 2011
6. Wikipedia. Minutiae-wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php 359363333, 2010.
7. Sun, D., Li, Q., Liu, T., He, B., and Qiu, Z.A secure multimodal biometric verification scheme. In Advances in Biometric Person Authentication, S. Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, and D. Zhang, Eds., vol. 3781 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2005, pp. 233-240.