Fingerprint based authentication application using visual cryptography methods (Improved ID card)

Mr. Y.V. Subba Rao, Ms. Yulia Sukonkina
Department of Computer and Information Sciences, University of Hyderabad, Gachibowli, Hyderabad, India
yvrcs@.uohyd.ernet.in, yulia_sukonkina@yahoo.com

Dr. Chakravarthy Bhagwati, Mr. Umesh Kumar Singh
Department of Computer and Information Sciences, University of Hyderabad, Gachibowli, Hyderabad, India
chakrcs@.uohyd.ernet.in, umeshsingh81@yahoo.com

Keywords: Visual Cryptography, Biometrics, Fingerprints, Authentication.

Abstract: **The main idea of this paper is to efficiently apply the Visual Cryptography (VC) techniques onto the area of authentication using fingerprints. We present an alternative approach of using the fingerprints, attempting to solve two major problems related to fingerprint based automatic access control systems which are falsification and the costly maintenance of the large fingerprint database. In the proposed application we divide an input fingerprint image into two shares with the help of the basic VC techniques, keeping one with the participant in the form of ID card and saving the other one in the database. This share kept in the database will be the same for all of the participants. While accessing, we will stack the corresponding shares together and compare the obtained image with the provided fresh fingerprint using any modern minutia extraction algorithm.**

1 INTRODUCTION

During the studies of multiple enhanced techniques in VC we found an interesting area to implement the existing ideas. Being aware of the certain issues concerning authentication control such as spoofing and "buddy punching" we are trying to introduce an application based on biometrics and an ID card in order to improve the security and cost of the overall admission process.

Our approach is to enable the completely synchronised combination of VC and the fingerprint scanner.

Considering fingerprint as a secret image we distribute it among the two shares following one of the advanced VC methods. First share is being a random image of the administrative database, whereas the second is the photograph on the ID card of the participant. We fix the same administrative share valid for all of the participants, hence utilising economically the size of the administrative database.

Being unbreakable VC assures the security of the both shares of the secret stored with the participants.

As long as VC does not require any computation during the decoding process, once the participant inserts his ID card and the corresponding share is extracted from it both shares participant's and administrative are simply superimposed to obtain the secret fingerprint image. From this image now the minutiae of the finger can be extracted.

On the next step the application requests the participant to render the new fingerprint. This image is processed by a system and the minutiae are extracted and compared with the minutiae of the secret fingerprint image obtained earlier.

Minutiae extraction and matching can be done with the help of any fingerprint scanner. The authentication succeeds only in case if minutiae are matching.

Overcoming the problems stated above our application does not reintroduce the problems associated with the non-biometric possession-based authentication techniques: that is, forgotten or guessed password, lost or stolen key, etc.

This paper is organized as following: Section 2 introduces a term biometrics; Section 3 and 4 summarizes the history of fingerprints and authentication process; Problems with the existing fingerprint readers are discussed in section 5; Introduction to Visual Cryptography and it's alternative presented in section 6 and 7; Section 8 describes the proposed application; Conclusions and future task are given in section 9.

Table 1: Comparison of Biometric Technologies.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F. Thermo-grams	High	High	Low	High	Medium	High	High

2 BIOMETRICS

Biometrics is the detailed measurements of the human body. Biometrics deals with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioural characteristics (S. Bistarelli et al., 2003). The most popular characteristics are fingerprints and facial features. A brief comparison of nine biometric techniques made by A. Jain et al. in 1997 is provided in Table 1.

3 FINGERPRINTS HISTORY

Definition: Fingerprints are graphical flow-like ridges present on human fingers (see Fig. 1). Their formations depend on the initial conditions of the embryonic mesoderm from which they develop (A. Jain et al., 1997).

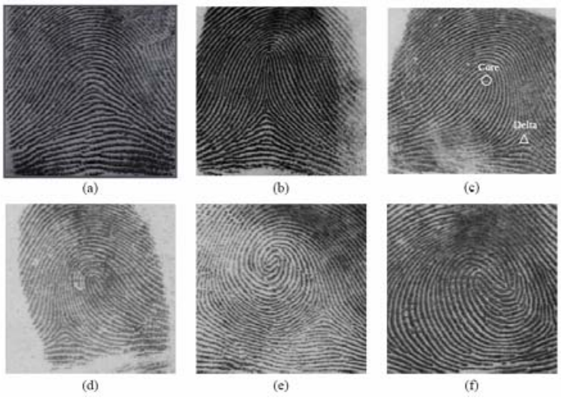

Fig. 1: A fingerprint classification schema of six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop; critical points in a fingerprint, called core and delta, are marked on image (c).

Modern fingerprint techniques were initiated in 1684 by English plant morphologist Nehemiah Grew. Starting from 1809, Thomas Bewick began to use his fingerprint as his trademark, which is believed to be one of the most important contributions in the early scientific study of fingerprint identification (A. Jain et al., 1997).

Later fingerprint identification systems were involved in criminal identification process. Nowadays these systems are widely used in multiple civil areas, such as in prevention of multiple enrollments in an electoral, welfare, custom control, employee attendance logging, security desk in banks, security installations, visitor verification, member verification in clubs, member organizations etc.

4 FINGERPRINT AUTHENTICATION PROCESS

In 2003 S. Bistarelli, G. Boffi and F. Rossi. In their paper “Computer Algebra for Fingerprint Matching” proofed that during fingerprint identification, it is desirable to have, at the least, a two stage search. The first stage makes use of global fingerprint characteristics while the second stage is the minutiae matcher (point pattern matching).

Authors state that typically, automatic fingerprint identification and authentication systems rely on representing the two most prominent structures: ridge endings and ridge bifurcations ((a) and (b) in Fig. 2 correspondingly). These two structures are background-foreground duals of each other and pressure variations could convert one type of structure into the other. Therefore, many common representation schemes do not distinguish between ridge endings and bifurcations. Both the structures are treated equivalently and are collectively called minutiae. The simplest of the minutiae-based representations constitute a list of points defined by their spatial coordinates with respect to a fixed image-centric coordinate system. Typically, though, these minimal minutiae-based representations are further enhanced by tagging each minutia (or each combination of minutiae subset, e.g., pairs, triplets) with additional features. For instance, each minutia could be associated with the orientation of the ridge at that minutia; or each pair of the minutiae could be associated with the ridge count: the number of ridges visited during the linear traversal between the two minutiae.

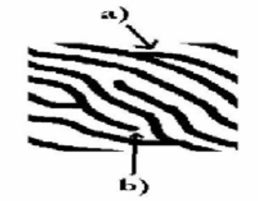

Fig. 2: An example of ridge endings b) and bifurcations a).

A feature extractor finds the ridge endings and ridge bifurcations from the input fingerprint images. If ridges can be perfectly located in an input fingerprint image, then minutiae extraction is just a trivial task of extracting singular points in a thinned ridge map. However, in practice, it is not always possible to obtain a perfect ridge map.

Finely, the researches have listed the stages required for the biometric authentication as following:

Capture: A raw biometric sample is captured by a sensing device, such as a fingerprint scanner or video camera.

Process: The distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (sometimes called biometric sample or biometric template).

Enrol: The biometric template is stored in a storage medium for comparison during an authentication phase. Notice that the original biometric sample cannot be reconstructed from this identifier.

Verification: In this mode (\1 to 1 matching"), a newly captured/processed biometric sample taken for instance during a login, is compared against a previously enrolled sample to address the question \Are you the person you claim to be?".

Identification: In this mode (\1 to N matching"), the individual does not claim an identity. The individual presents a biometric sample and the system tries to identify the individual from a database of stored biometric samples.

5 PROBLEMS WITH THE EXISTING FINGERPRINT READERS

The performance of currently available minutiae extraction algorithms depends heavily on the quality of input fingerprint images. Due to a number of factors (aberrant formations of epidermal ridges of fingerprints, postnatal marks, occupational marks, problems with acquisition devices, humidity and ageing of the finger etc.) fingerprint images may not always have well-defined ridge structures (A. Jain et al., 1997). For example, paper of A. Jain et al. shows the development of a new algorithm for fingerprint matching able to take care of translations, rotations and other transformations. The algorithm is also able to match fingerprints when some minutiae are missed or when some unreal minutia is detected. But unfortunately none of these algorithms is infallible. However, the rates of false negatives and false positives have markedly improved. One of the significant problems with fingerprint readers, for instance, is that they couldn't distinguish between an actual fingerprint and the image of one. Some fingerprint scanners can be spoofed with nothing more than a breath of hot air, which reactivates latent prints left on the scanner.

The solution of these problems is provided by the higher-end fingerprint readers, which are expansive. The latest fingerprint readers are incorporating more advanced features, such as making sure the finger is a certain temperature, a pulse and pressure. Such sophistication, however, has its drawbacks. Authorized users may find themselves locked out even when the devices are working properly, because of tiny changes, due to accidents or injuries, which can change a biometrics profile, rendering it effectively obsolete.

Biometric authorization techniques are no longer so leading edge that they are difficult to marry with traditional security safeguards. A strong authentication system is what we want to focus on and biometrics can be a part of it, but the user should still have to memorize something or have a token, and we need to make sure that polices and the management structure relating to it are firmly in place.

Such a solution we find using Visual Cryptography methods along with Fingerprint Based Access Control System.

6 INTRODUCTION TO VISUAL CRYPTOGRAPHY

In 1995 Naor and Shamir have suggested for the first time to solve the secret sharing problem by the means of new cryptographic structure called Visual Cryptography (VC). In the proposed approach the secret is divided into two shares, which are printed onto the two transparencies (shares) and given to the participants. Only these two participants who possess the transparencies can reconstruct the secret by superposition of shares. One can not recover a secret without the other one.

In the visual threshold scheme, the shares are images represented on transparencies consisting of black and white (transparent, actually) pixels. The visual systems perform a Boolean OR operation, which is easy to visualise using the (2, 2) Visual Threshold Scheme shown in Fig. 3.

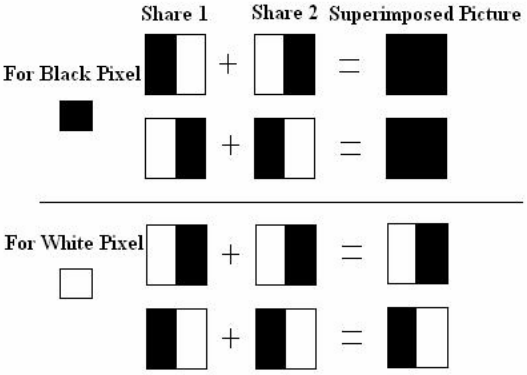

Fig. 3: (2, 2) Visual Threshold Scheme.

Later in 2001 the engineers from Taiwan in their paper (C.S. Tsai et al., 2001) have claimed that during the encoding process shares are generated in such a way that they contain random dots to create a chaos for preventing intruders of random guesswork. This leads to a trouble of stacking the dots with each other. However the problems of disorderliness and unstackability can be eliminated using a multiple secret sharing method, which adds a small amount of computation. They propose two algorithms for secret sharing and secret recovery derived from the least significant bit substitution method. They convert the secret into many bit planes and modify the so called cover images based on these bit planes. Each modified cover image is called stego-image.

Thus generation of shares could be also done using so called cover images. In the next section we will explain this alternative algorithm for creating shares used by Tsai, Chang and Chen.

7 Alternative Way Of Share Generation Introduced By Tsai Et Al.

Assume there are two participants $\{n_1\}$ and $\{n_2\}$ and two digital grayscale cover images C_1 and C_2. Suppose $S = s_1\ s_2\ s_3 \dots s_t$ is the selected secret image. Here s_i is the i-th bit of S and the bit length of S is t, where:

$$t \leq min\ (C_1\ size,\ C_2\ size) - 16 \qquad (1)$$

If this condition is satisfied, next goal is to find two bit planes in cover images and apply them to share the secret.The bit planes are generated as depicted in Fig. 4. The maximum number of bit planes in one cover image equals to eight (i.e. 8 bits in a byte).

According to Fig. 4 C_i is i-th bit plane of cover image C. C_i [j] is the j-th bit of the i-th bit plane of C.

Each bit plane can be applied to share two secret messages with two different participants. This indicates an economical utilization of bit planes, implying that a small number of bit planes may keep a great number of secrets to be shared.

Each first 16 bits of the bit plane are used for the identification purpose and help to manipulate the bit planes efficiently. Here a_i is the 1st eight bits of each bit plane C_i and b_i is the next eight bits. Initially a_i and b_i are set to be zero, which indicates that C_i have not yet been applied to share any secret. There are nodes identification numbers N_1 and N_2, which are set to be any number greater then zero.

To find two bit planes all indicators in both C should be scanned to find min value of i, s.t. a_i is not equal to zero and b_i is equal to zero. This indicates that this bit plane is occupied to share secret with one participant, its' contents was used and can't be modified any more. If this condition doesn't exits in C then value of i is set to be -1 and the selection process continues.

Note that each secret bit s_i corresponds with one bit of the selected bit plane.

After selecting the bit planes from the cover images, two random permutations are generated. The size of these permutations is the same size as the secret. The bits of the bit plane starting from 16th are permuted with the original secret according to the generated permutation.

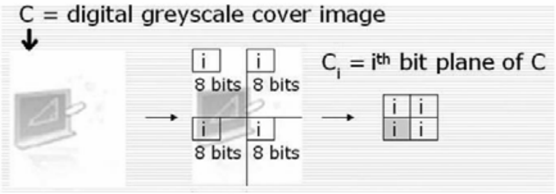

Fig. 4: Bit plane extraction.

Permuted bits of the bit plane should satisfy the following equation and reproduce s_i:

$$s_i = C'^{\,i}_{x}[per_x(k)+16]\ XOR\ C'^{\,j}_{y}[per_y(k)+16] \qquad (2)$$

where $1 \leq k \leq t$, $C'^{\,i}_{x}$, $C'^{\,j}_{y}$ are the i-th and j-th bit planes of the C'_x and C'_y modified cover images correspondently.

Hence during recovery of the secret bits we have to obtain both modified cover images, scan them to find and extract the bit planes used for the secret sharing. Then the Equation 2 has to be applied on each bit of the bit plane one after the other stepwise reconstructing the secret.

Next section explains the idea of embedding these secret sharing and recovery algorithms into the Automated Fingerprint Authentication System.

8 Proposed Application

Assume we require assembling the Automated Fingerprint Identification System on the entrance of the secret building. The administrator will collect the fingerprints of the people eligible to enter the building. She will consider each fingerprint as a secret image. Randomly a unique dummy share will be created and saved securely in the database. The shares of the participants will be created from this dummy share and the fingerprint images with the help of standard VC methods or any other VC sharing algorithms. For the better security we will embed the share of the participant into her cover image, which is a photograph on her ID card. There are multiple papers proposed which are referring to how to use the cover images during the secret sharing process. For example, in section 7 we have described one of them.

The participant share will be permuted using the random permutation, which will be unique for each participant. For generating the random permutation the Random Number Generator is required. On the other hand we "recall that computers can't create real random numbers, just streams of numbers that appear random to the outside observer" (P. Johnson et al., 2000). But random numbers are often initialized using a computer's real time clock as the seed. These functions may provide enough randomness for the certain tasks. Much higher quality random number sources are available on most operating systems; for example /dev/random on various BSD flavors, Linux, Mac OS X, IRIX, and Solaris, or CryptGenRandom for Microsoft Windows. Random number generators are very useful as debugging is facilitated by the ability to run the same sequence of random numbers again by starting from the same seed. They are also used in cryptography so long as the seed is secret. Sender and receiver can generate the same set of numbers automatically to use as keys.

In our application the administrative database will store the integer seed which will be used to generate the set of the required random permutations. Thus we will avoid the problem of storing large sequences of random numbers in our database. Moreover the shares of the participants will be stored in their ID cards and the administrator will have to maintain the database where only the dummy share and the integer seed will be stored.

For entrance the participant will provide her share in the form of ID card, which will be met by the system. Using the reverse permutation, dummy share and applying the VC techniques system will generate the image of the fingerprint provided by the participant during the registration. This image will be compared with the newly provided fingerprint using any of the modern minutiae extraction algorithms. If the results of the comparison will match, entrance will be allowed, as shown in Fig. 5.

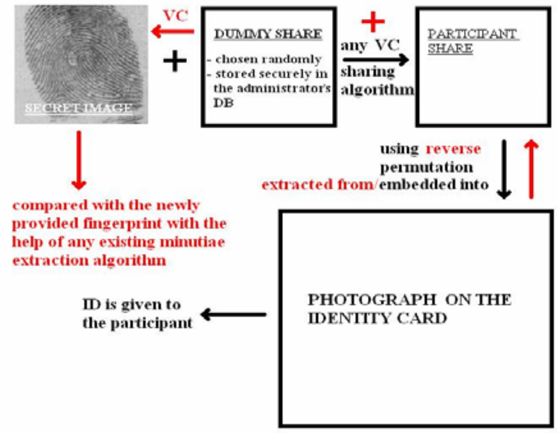
VC
SECRET IMAGE
+
DUMMY SHARE
- chosen randomly
- stored securely in the administrator's DB
+
any VC sharing algorithm
PARTICIPANT SHARE
using reverse permutation
extracted from/embedded into
compared with the newly provided fingerprint with the help of any existing minutiae extraction algorithm
ID is given to the participant
PHOTOGRAPH ON THE IDENTITY CARD

Fig. 5: Registration and authentication process.

9 CONCLUSIONS AND FUTURE PLANS

Looking back to the existing problems with fingerprint readers we achieve the following results:

- There is no more problem with the falsification of the finger, because the entrance will succeed only in case if the participant will provide the ID card.
- There is no need for the administrator to maintain a large data base of the fingerprints.

We overcome the problems stated above without reintroducing the problems associated with the non-biometric authentication techniques. These security problems inherent in the knowledge- and possession-based techniques: that is, a password can be forgotten or guessed, a key may be lost or stolen, and both can be shared (D. Maltoni, 2003).

We affirm that the cost difference of the techniques involved in our application is negligible as in compare with techniques used by the existing Fingerprint Based Authentication Systems. Moreover it is luckily slightly reduced. The statistical cost analysis is our future task.

REFERENCES

[1] Noar M., Shamir A., 1995. Visual cryptography. Advances in Cryptography. *Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag. 1 – 12.*

[2] Tsai C.S., Chang C.C., Chen T.S., 2001. Sharing multiple secrets in digital images. *Department of Computer Science and Information Engineering, Taiwan. 1 – 8.*

[3] Subba Rao Y.V., 2007. Presentation on Visual Cryptography and Its Applications. *Department of Computer and Information Sciences, University of Hyderabad, India. 1 – 42.*

[4] Jain A., Hong L., Pankanti S., Bolle R., 1997. An Identity Authentication System Using Fingerprints. *Department of Computer Science, Michigan State University, USA. 1- 66.*

[5] Bistarelli S., Boffi G., Rossi F., 2003. Computer Algebra for Fingerprint Matching. *Universita "G. d'Annunzio", Dipartimento di Scienze, Pescara, Italy. 1 – 10.*

[6] Davide Maltoni 2003. Handbook of Fingerprint Recognition. 1 – 366.

[7] Swarm Development Group, Johnson P., Lancaster A., 2000. Swarm User Guide. 1 – 176.

[8] Stinson D.R., Tavares S., 2000. The Pseudo-Random Number. Selected Areas in Cryptography. *7th Annual International Workshop, Waterloo, Ontario, Canada. 100 - 101.*

[9] http://www.ravirajtech.com/biometrics_news.html

[10] http://www.bioenable.com/usb_fingerprint_time_attendance_india.htm

[11]http://www.webopedia.com/DidYouKnow/Computer_Science/2006/biometrics_security.asp

[12]http://en.wikipedia.org/wiki/Automated_Fingerprint_Identification_System

[13] http://en.wikipedia.org/wiki/Random_number_generation