International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Design of Protection in Iris Biometric Recognition Using Watermarking Technology

P.Srilatha

Abstract: In order to handle this problem, researches have proposed dissimilar algorithms to be challenged by security of biometric systems. Two major ways are, (1) Encryption, and (2) watermarking by securing biometric images and templates. In this project, we utilize a watermarking technology to improve the template security in biometric authentication. According to, two modalities such as, iris and hand vein is taken to preserve the characteristics of liveliness and permanency. The existing technique of embedding of iris data to hand vein images using watermarking technology consist of following steps, i) preprocessing of iris and hand vein images, ii) iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images. After this the extracted iris template was embedded in to the hand vein and stored in the database. Subsequently in recognition phase the iris template and hand vein features were extracted from the watermarked image. Finally the extracted features were matched with input query image.

Keywords- Template, Fingerprint, watermarking, embedding, extraction and authentication.

I. INTRODUCTION

Biometrics is a technology that uses physiological or behavioral characteristics to authenticate identity of persons. For automated personal identification biometric authentication is getting more attention. There are various application where personal identification is required such as passport control, computer login control, secure electronic banking, bank ATM, credit cards, premises access control, border crossing, airport , mobile phones, health and social services, etc. Many biometric techniques are available such as facial thermo gram, hand vein, gait, keystroke, odor, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature. Among those iris recognition is one of the most promising approach because of stability, uniqueness and noninvasiveness. Biometrics systems are more consistent and more user friendly. Still there are certain issues particularly the security facet of both biometric system and biometric data. As template is stored in centralized database, they are vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be considered. For these reasons various researches have been made to protect the biometric data and template in the system by using cryptography, Stegnography and watermarking. In this paper a system is proposed by applying visual cryptography technique to biometric template (iris). Visual cryptography technique has been applied on to the iris template to make it secure from attack in centralized database as well as extra layer of authentication to the users

A. Background

Advanced Watermarking depicts techniques and innovations that conceal data, for instance a number or content, in computerized media, for example, pictures, video. The inserting happens by controlling the substance of the advanced information, which implies the data is not installed in the casing around the information. The concealing procedure must be to such an extent that the alterations of the media are vague. For pictures this implies the alterations of the pixel values must be imperceptible. An advanced watermark is a message which is installed into computerized content (video, pictures or content) that can be identified or extricated later. In addition, in picture the genuine bits speaking to the watermark must be scattered all through the document such that they can't be distinguished and controlled. Watermarking is the addition of indistinct and indistinguishable data into the host information for information security and uprightness. There are portraying examples, of differing perceivability, added to the introduction media as a certification of

realness, quality, possession, and source. The most widely recognized case of watermark is an Indian cash.

B. History:

More than 700 years back, watermarks were utilized as a part of Italy to show the paper mark and the factory that created it. By the eighteenth century watermarks started to be utilized as Anti-duplicating measures on cash and different archives. The term watermark was presented close to the finish of the eighteenth century. It was presumably given on the grounds that the imprints look like the impacts of water on paper. The main case of an innovation like computerized watermarking is a patent documented in 1954 by Emil Hem Brooke for recognizing music works. In 1988, Komatsu and Tominaga give off an impression of being the first to utilize the expression "advanced watermarking". Digital watermarks are of four types:

1) Visible

2) Invisible

3) Public, and

4) Fragile

A visible watermark regularly comprises of a prominently noticeable message or an organization logo showing the responsibility for picture. Any evacuation or messing with the logo would break the copyright understanding.

An invisible watermarked picture seems fundamentally the same as the first. The presence of an undetectable watermark must be resolved utilizing a proper watermark extraction or location calculation. It can be identified by an approved office as it were. Such watermarks are utilized for substance and additionally creator validation and for distinguishing unapproved copier.

C. Iris Recognition

Iris acknowledgment is a robotized strategy for biometric distinguishing proof that utilizations scientific example acknowledgment methods on video pictures of either of the irises of a person's eyes, whose intricate irregular examples are one of a kind, stable, and can be seen from some separation. Retinal filtering is an alternate, visual based biometric innovation that uses the interesting examples on a man's retina veins and is frequently mistaken for iris acknowledgment. Iris acknowledgment utilizes camcorder innovation with inconspicuous close infrared brightening to procure pictures of the detail-rich, unpredictable structures of the iris which are obvious remotely. Computerized layouts encoded from these examples by scientific and factual calculations permit the recognizable proof of an individual or somebody putting on a show to be that person. A key preferred standpoint of iris acknowledgment, other than its speed of coordinating and its outrageous imperviousness to false matches is the soundness of the iris as an inner and ensured, yet remotely obvious organ of the eye.

D. Visible Wavelength(VW) v/s Near Infrared Rays(NIR)

All freely sent iris acknowledgment frameworks obtain pictures of an iris while being enlightened by light in the close infrared wavelength band (NIR: 700–900 nm) of the electromagnetic range. The lion's share of people worldwide have "dim dark colored eyes", the prevailing phenotype of the human populace, uncovering less noticeable surface in the VW band however showing up luxuriously organized, similar to the cratered surface of the moon, in the NIR band. (A few cases are appeared here.) Using the NIR range likewise empowers the obstructing of corneal specular reflections from a brilliant surrounding condition, by permitting just those NIR wavelengths from the limited band illuminator once more into the iris camera.

Protecting the template is a challenging task in the biometric system (attack on point 6). Many researchers have been made to protect fingerprint and iris data and template. Davida at al, make the use of error-correcting codes in designing a secure biometrics system for access control. Following the work, Juels and Wattenberg broaden the system by establishing a different way of using error-correcting codes and approach is known as “fuzzy commitment”. Chander Kant et al, presented the idea

for biometric security using Stegnography to make system more secure. While encoding the secret key (which is in the form of pixel intensities) will be merged in the picture itself, and only the authentic user will be allowed to decode. Khalil Zebbiche et al, proposed wavelet based digital watermarking method to hide biometric data (i.e. fingerprint minutiae data) into fingerprint images. This provides a high security to both hidden data (i.e. fingerprint minutiae) that have to be transmitted and the host image (i.e. fingerprint).

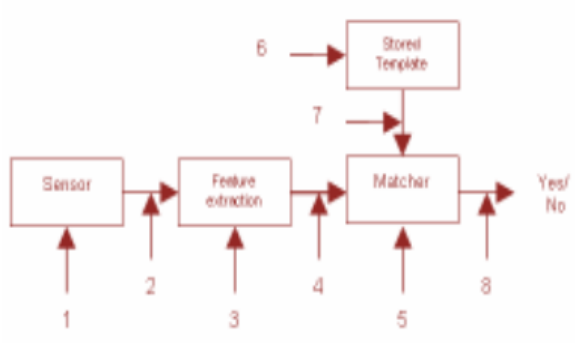

Fig.1. Possible attack points in generic biometric systems

To protect fingerprint images presented an efficient technique for use in fingerprint images watermarking. The underlying principle of the technique is embedding the watermark into the ridges area of the fingerprint images which represents the region of interest. The viability of templateprotected biometric authentication systems was exhibited with a fingerprint recognition system by introduced an amplitude modulation-based watermarking method in which they hide a user's biometric data in a variety of images. By combining asymmetric digital watermarking and cryptography as a powerful mechanism was proposed by Nick Bartlow et al, to store raw biometric data in centralized databases. Shenglin Yang et al, presented a template protected secure iris verification system based on the Error Correcting Code (ECC) cryptographic technique with the reliable bits selection to improve the verification accuracy. In the scheme a transformed version of the iris template instead of the plain reference is stored for protecting the sensitive biometric data. Jing Dong et al, proposed biometric watermarking for protecting biometric data and templates in biometric systems. The scheme suggest protection of iris templates by hiding them in cover images as watermarks (iris watermarks), and protection of iris images by watermarking them.

II. PROPOSED SCHEME

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

i) Fingerprint Recognition
ii) Fingerprint Patterns
iii) Embedding Of Iris Pattern to Fingerprint Image
iv) Watermark Extraction

i) Fingerprint Recognition

Human fingerprints have been discovered on a large number of archeological artifacts and histological items. Although these findings provide evidence to show that ancient people were aware of the individuality of fingerprints, it was not until the late sixteenth century that the modern scientific fingerprint technique was first initiated (Jain, et al, 2003). Every person's fingerprints are unique, and will always maintain their uniqueness explaining why they have been used for many years for authentication purposes. For example, the FBI fingerprint identification division was set up, in 1924, with a database of 810,000 fingerprint cards (Federal Bureau of Investigation, 1984).In 1890, Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals.

ii) Fingerprint Patterns

A fingerprint consists of three basic patterns of ridges, the arch, loop and whorl as shown in Figure 2. An arch can be explained as the pattern where ridges begin from one side of the finger, ascent in the centre

which develops an arc, and then exits the finger from the opposite side. A loop can be explained as the pattern where ridges begin at one side of a finger to create a curve, and are inclined to exit in the same way they entered.

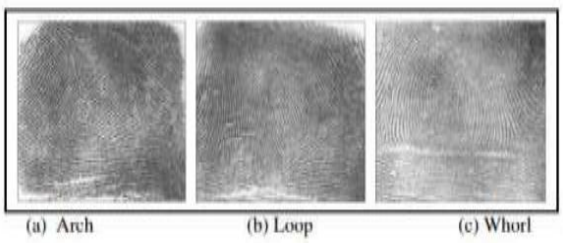

Figure 2. Basic Patterns of Fingerprint

As seen above in Figure 2(c), in the whorl pattern, ridges are structured in a circular position around a central spot on the finger. In general, researchers have discovered that relatives frequently share similar fingerprint patterns, which has led to the concept that fingerprint patterns are genetic.

iii) Embedding of Iris Pattern to Fingerprint Image

l) The input watermark image F(x,y)is divided into blocks of B1,B2,B3, ...Bn of size MxN. Then the divided block is sorted. From the sorted block of the input image F(x,y) the first wavelet coefficient with positive phase and the value below the threshold T(x,y) is chosen.

2) Then the second LSB of the selected block of the watermark image F(x,y)is replaced by one bit from the iris template I(x,y).

3) If the number of bits in the iris template I(x,y) is less than the number of blocks in fingerprint image, then all bits of the iris template I(x,y) can be embedded.

4) After embedding all the bit of the iris template I(x,y) in fingerprint image an IDWT (Inverse Discrete Wavelet Transform) is applied to the watermarked fingerprint coefficient to generate the final secure watermarked fingerprint image. The watermark embedding process is shown in the figure below,

iv) Watermark Extraction

The watermark extraction phase consists of various steps:-

The input is watermarked image FW(x,y) and the size of watermarked image FS(x,y) and the output is recovered watermark image RW (x, y).

1) The watermarked image is divided in to the detail sub band of watermarked image in to blocks. The each block of the watermarked image is of size 2M -1 x 2N -1 .

2) Identify the value below the threshold T(x,y) in each block which has the first coefficient with positive phase.

3) The pixel value 1 from the watermarked image is extracted if the embedded pixel value is greater than the mean pixel value otherwise pixel value '0' is extracted.

4) A matrix equal to the size of watermark image FW(x,y) and the extracted pixels are placed in it to obtain the watermark image Fs' (x,y) .

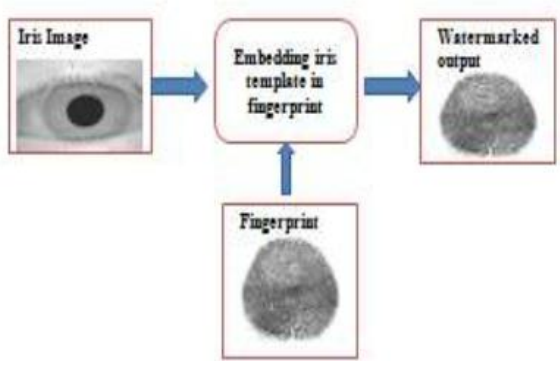

Figure 3. Fingerprint watermark Embedding

In recognition phase the both iris and fingerprint image of an individual is taken. Then both the obtained iris image and the fingerprint image are separately as by the above procedures. The iris key is embedded in the fingerprint image to improve the template protection. So here we have to extract the iris key and fingerprint separately.

III. SIMULATION RESULTS

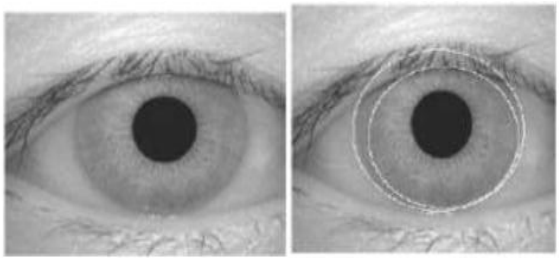

Figure (Existed) 4(a). Original Iris Image Figure 4(b). Iris Image with Boundaries

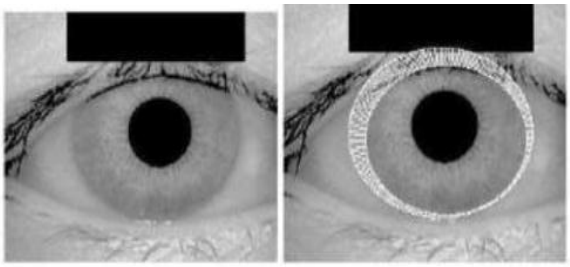

Figure (Existed) 4(c). Segmented Iris image Figure 4(d).Segmented Iris image with Boundaries

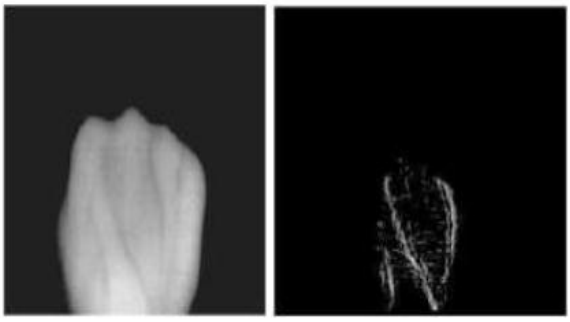

Figure. 5(a). Original hand vein Image Figure.5 (b). Extracted vein image

Figure. 5(c). Watermarked hand vein image

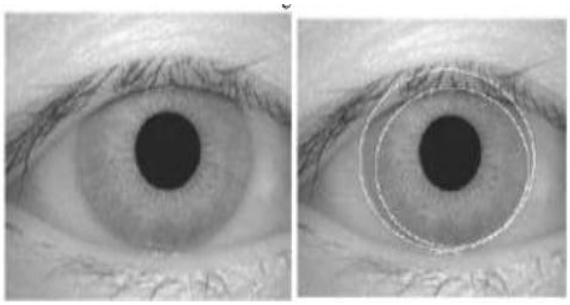

Figure (proposed) 6(a). Original Iris Image Figure 6(b). Iris Image with Boundaries

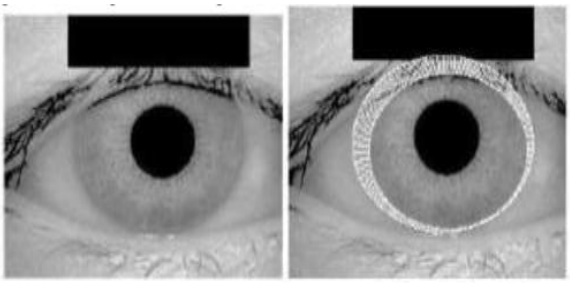

Figure (proposed) 6(c). Segmented Iris image Figure 6(d).Segmented Iris image with Boundaries

IV. CONCLUSION

We have used a watermarking technology to improve the template protection based on the two modalities the iris and the hand vein. The iris template was extracted from the pre-processed iris image. Then the features of the hand vein were extracted. After this the extracted iris template was embedded in to the hand vein and stored in the database. Subsequently in recognition phase the iris template and hand vein features were extracted from the watermarked image. Fingerprint features are real human physiological characteristics, unique, permanent and not changeable. However, biometric characteristics are not secret and fake fingerprint image can be reconstructed easily. Therefore, fingerprint sample cannot be trusted for unattended-based authentication applications. The proposed method can be further improving the Accuracy by considering the embedding the iris data to fingerprint images using watermarking technology for template protection.

REFERENCES

[1] R. Yadav, Kamaldeep, R. Saini, and R. Nandal, "Biometric Template security using Invisible

Watermarking With Minimum Degradation in Quality of Template," International Journal on Computer Science and Engineering, vol. 3, no. 12, 2011.

[2] J.L. Jimenez, R.S. Reillo and B.F. Saavedra, "Iris Biometrics for Embedded Systems," IEEE Transactions on Very Large Scale Integration (VLSI) systems, vol. 19, no. 2,2011.

[3] P.S. Revenkar, A Anjum and W.Z. Gandhare, "Secure Iris Authentication Using Visual Cryptography," International Journal of Computer Science and Information Security, vol. 7, no.3, 2010.

[4] AK. Jain, A Ross, and U. Uludag, "Biometric Template Security Challenges and Solutions," In Proceedings of European Signal Processing Conference, 2005.

[5] N. Hajare, A Borage, N. Kamble, and S. Shinde, "Biometric Template Security Using Visual Cryptography," Journal of Engineering Research and Applications (IJERA), vol. 3, no. 2, pp. 1320-1323,2013.

[6] C.L. Li, Y.H. Wang, and B. Ma, "Protecting Biometric Templates using LBP-based Authentication Watermarking," Chinese Conference on Pattern Recognition, pp. I -5,2009.

[7] Salil Prabhakar, Sharath Pankanti, and Anil K Jain. Biometric recognition: Security and privacy concerns. IEEE Security&Privacy, 1(2):33-42, 2003.

[8] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In ElectronicImaging2002, pages 275-289.InternationalSocietyforOpticsand Photonics, 2002.

[9] P. Poongodi, and P. Betty, "A Study on Biometric Template Protection Techniques," International Journal of Engineering Trends and Technology (IJETT), vol. 7, no. 4, 2014.

[10] K. Seetharaman, and R. Ragupathy, "Iris Recognition based Image Authentication," International Journal of Computer Applications, vol. 44, no. 7,2012