A Fingerprint Watermarking Algorithm to Enhance The Privacy Of Fingerprint Data

Sandhya Tarar, Ashish Kumar, Ela Kumar
School of ICT,
Gautam Buddha University,
Greater Noida,
India
tarar.sandhya@gmail.com, ashih@gmail.com, elaku@gmail.com

Abstract

Digital watermarking of fingerprint images has been explored to solve the problems of security of data. Biometric data security concerns are receiving the widespread public acceptance of biometric technology. Since a number of security mechanism have been proposed, but due the trade-off between identification efficiency and security of stored template, practical applications have not benefited up to desired level. In this paper, we have designed a watermarking algorithm to improve the recognition performance as well as the security of a fingerprint based biometric system. The proposed algorithm provides the effective solution of security issues regarding biometrics techniques without affecting the fingerprint quality. We have used fingerprint Verification Competition 2004 (FVC 2004) as a database for implementation of proposed algorithm. Experimental results show the efficacy of our algorithm.

Keywords: Fingerprint Digital Watermarking, Biometric Technology, Fingerprint Identification System (FIS), Electronic Watermark, Fingerprint Verification Competition (FVC)

1. Introduction

In recent years, the digital transmission of biometric data has introduced flexible, cost effective communication models that are beneficial in various transactions. At the same time, they also possess some serious drawbacks that digital data can be duplicated very easily without introducing any quality degradations to the content. Digital watermarking is a technique that is used to solve this problem. This does not allow an individual, other than the owner, to manipulate, duplicate, or access media information without owner's permission. This inspires a lot of research efforts in digital watermarking of biometrics. Fingerprint recognition is significance identification method among the various identification techniques and we are working on it in order to increase the degree of security with the help of watermarking technique. Andrew Tirkel and Charles Osbome introduced "digital watermark" term in 1992 [41]. "Digital watermarking" is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents without affecting the overall quality of the original content [1]. Digital watermarks are electronic way to embed the information on any multimedia content. Digital watermarks are used to uniquely identify the image in order to claim for the original content/image. These watermarks may be in form of text or image. In this paper we have used text watermark and embed on fingerprint images to make an appropriate belongingness or authentication. Thus, it is used to provide the security of contents in form of data protection. Watermarking techniques can be classified into differenet categories. Broadly these techniques can be classified into four areas according to the type of place to be watermarked as follows. Watermarking on images is called as image watermarking, if one apply watermark on videos referred as video watermarking, watermarking of audio signal come under the heading of audio watermarking and if watermarking has been applied on text this is called as text watermarking [30]. If we want to classify according to the human perception, the digital watermarks can be divided into three different types as follows. Visible watermark: - The information is visible in the picture or video. Typically, the information is text or logo, which identifies the owner of the media. Invisible-Robust watermark: - if the watermarked content is equivalent to the original, un-watermarked content it is easy to create robust watermarks—or—imperceptible watermarks, but the creation of robust—and—imperceptible watermarks has proven to be quite challenging. Invisible-Fragile watermark: - it is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. From application point of view digital watermark can be classify as Source based or Destination based. Source based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. Destination based watermark can be used to trace the buyer in the case of illegal reselling [30].

2. Previous Work

According to A. Z. Tirkel et al. [1], discuss the feasibility of coding a robust, undetectable, digital watermark on a standard 512*512 intensity image with an 8 bit gray scale. It is possible to embed this information on images in order to provide higher degree of authentication. This possibility leads to use images for more applications such as image tagging etc. and provide control access. The method chosen is based on linear addition of the watermark to the image data. Brassil et al. [4], have investigated different methods for marking text within documents with a unique binary codeword which serves to identify legitimate users of the document. The codeword is embedded in a document by making subtle modification to the structure of the document such as modulation of line width and interword spacing as well as modification of character fonts. Walton [5] has developed a technique for introducing checksums in the last significant bits of an image to implement a fragile watermark and thus prevent unauthorized tampering. Chang-Hsing Lee et al. [6], proposed an adaptive digital image watermarking technique. The proposed method exploits the sensitivity of human eyes to adaptively embed a visually recognizable watermark in an image without affecting the perceptual quality of the underlying host image. The watermark will still be present if some lossy image processing operation such as low –pass filter, resampling and lossy JPEG image compression are applied to the watermarked image. J.J.K. O Ruanaidh et al. [7], an embedded watermark should be visually imperceptible, secure, reliable and resistant to attack. They describe the method to fulfill the requirements: imperceptible – the image must not be visibly degraded by the presence of the mark. The mark should serve as a unique identifier with high information content. Secure and reliable – the mark must be strongly resistant to unauthorized detection and decoding. The watermark must also be capable of identifying the source and intended recipient with a low probability of error. It is also desirable that it would be difficult for an Innovative error-control coding and digital signature techniques are required to ensure reliable and secure communication of the mark as well as authentication of the encoded message. Robust – the mark must be robust to attack and must be tolerant to reasonable quality lossy compression of the image using transform coding or any other technique. Ms. D. Mathivadhani and Dr. C. Meena [8], considers two techniques that protects of fingerprint biometric data using digital watermarking techniques. Both techniques are discussed based on Discrete Wavelet Transformation (DWT). This paper discusses two fingerprint watermarking systems, referred to as Zebbiche et al., 2009 given Model-1 and Vatsa et al., 2006 provided Model-2. The primary objective of both the models is to protect fingerprint images during transmission using watermarking techniques. According to A. Z. Tirkel et. al. two basic classes exist of electronic watermarks: fragile and robust. In recent explosion in digital communications and the rapidity and ease of transmission of electronic material which is subject to copyright. The authors have been concerned with the construction of the robust type which is resilient to some image distortions such as pixel or bit tampering, cropping, translation and rotation [1]. The codeword is embedded in a document by making suitable modifications to the structure of the document such as modulation of line width and character fonts. Standard document handling operations such as photocopying and scanning do not remove the watermark [4].

According to Jana Dittmann *et al.,* Digital watermarking is the enabling technology to prove the belongingness to copyrighted material, detect originators of illegally made copies, monitor the usage of the copyrighted multimedia data and analyze the spread spectrum of the data over networks and servers. Embedding of unique customer identification as a watermark into data unauthorized agent to forge watermarks. is called fingerprinting to identify illegal copies of documents. Basically, watermarks embedded into multimedia data for enforcing copyrights must uniquely identify the data and must be difficult to remove, even after various media transformation processes. Digital fingerprinting raises the additional problem that we produce different copies for each customer. Attackers can compare several fingerprinted copies to find and destroy the embedded identification string by altering the data in those places where a difference was detected. The only marking positions the pirates cannot detect are those positions which contain the same letter in all the compared documents, called intersection of different fingerprints. In our paper we described a water marking scheme to embed customer information into images in form of text to avoid unauthorized access. Current digital fingerprinting has the disadvantage, that customers could work together as attackers to destroy the watermarking information by comparing their image data and remove the differences. With our proposed technique attackers could still work together, but our mechanisms provide the possibility to conclude to the customers which attacked the watermark. Our robustness tests of the watermarking scheme based on DCT coefficients are mainly based on compression, format conversions and geometrical transformations. Format conversions are handled with very low error rates. The fingerprinting tests, comparing different image copies, are successful and the remaining intersection gives the possibility to trace the attackers. Altogether our tests show that the watermarking technology with special marking points is satisfying.

According to Jianjiang Feng *et al.*, Fingerprint matching systems generally use four types of representation schemes: grayscale image, phase image, skeleton image, and minutiae, among which minutiae-based representation is the most widely adopted one. The compactness of minutiae representation has created an impression that the minutiae template does not contain sufficient information to allow the reconstruction of the original grayscale fingerprint image. This belief has now been shown to be false; several algorithms have been proposed that can reconstruct fingerprint images from minutiae templates. These techniques try to either reconstruct the skeleton image, which is then converted into the grayscale image, or reconstruct the grayscale image directly from the minutiae template. However, they have a common drawback: Many spurious minutiae not To overcome the security issues regarding fingerprints identification, fingerprint watermarking is considered as an effective technique. For this purpose, we proposed an algorithm in order to enhance the degree of privacy of fingerprint data. This paper discusses the algorithm design, implementation and experimental results. The main objective of this algorithm is to protect fingerprint images with the help of watermarking techniques. Proposed algorithm is used to embed the watermark within the fingerprint image. Details of the proposed algorithm are given below.

3.1 Proposed Algorithm

The BufferedImage provides way to manipulate the Image data. There are two components of a BufferedImage object, one is ColorModel object and another is Raster object. The ColorModel object provide methods that translate an image's pixel data into color component such as RGB for a computer. The Raster represents a rectangular array of pixels. The sample values and a SampleModel that describes how to locate a given sample value in a DataBuffer combinely strored in a DataBuffer. The Raster holds a DataBuffer, which contains the raw image data and a SampleModel, which describes how the data is organizesinthebuffer.

included in the original minutiae template are generated in the reconstructed image. Moreover, some of these reconstruction techniques can only generate a partial fingerprint. In this paper, a novel fingerprint reconstruction algorithm is proposed to reconstruct the phase image, which is then converted into the grayscale image. The proposed reconstruction algorithm not only gives the whole fingerprint, but the reconstructed fingerprint contains very few spurious minutiae. Specifically, a fingerprint image is represented as a phase image which consists of the continuous phase and the spiral phase (which corresponds to minutiae).

Algorithm for text watermarking of fingerprint images

Step1 -*Load an image to the BufferedImage using "java.awt.image.Image" interface, a BufferedImage is an*
accessible buffer of image data, essentially pixels, and their RGB colors.
"BufferedImage bi=new BufferedImage(icon.getIconWidth(),icon.getIconHeight(), BufferedImage.TYPE_INT_RGB)"

Step2 –*Cast the Graphics object to a Graphics2D object with this tool.*
"Graphics2D g2d= (Graphics2D) bufferedImage.getGraphics()"

Step3 – *Draw the image on the screen.*
"g2d.drawImageIicon.getImage(),0,0,nfull)"

Step4 –*By using the "setComposite(Composite rule)" method specifies how the pixels of a new shape are combined with the existing background pixels. Second approach to set the alpha value associated with composite rule, which control the transparency of the shape. By default, the transparency value is 1.0f (opaque).*
"AlphaComposite alpha = alphaComposite.getInstance(AlphaComposite. SRC_OVER, 0.6f)"

Step5 –By *using Graphics2D object, draw the Text or String on BufferedImage.*

"g2d.drawString(watermark_text, icon.getIconWidth()/2, icon.getIconHeight()/2)"

Abstract Windowing Toolkit (AWT) include limited available fonts, lines drawn with single-pixel width, shapes only in solid colors. The Java 2D API provides a robust package of drawing tools to develop high-quality graphics. Colors and patterns can be painted with color gradient and fill patterns. Transparent drawing of a shape is controlled through an alpha composite transparency value. Transformation of the coordinate system translations, scaling and rotations are available. The paint component method is supplied with a Graphics2D object.

3.2 Algorithm Implementation

To Import the java package to load an image into bufferedimage:

```
import javax.imageio.*;
import java.awt.image.*;
To load an image:
ImageIcon icon;
 icon=new ImageIcon(“ref.jpg”);
BufferedImage bdi;
bid=new
BufferedImage(icon.getIconWidth(),
icon.getIconHeight(),BufferedImage.TY
PE_INT_RGB);
To draw an image on the screen:
to draw an image on the panel using
graphics2d.
Graphics2D g2d;
g2d=(Graphics2D) bdi.getGraphics();
g2d.drawImage(icon.getImage(), 0, 0,
null);
To set the transparency using
setcomposite method:
int ac;
ac = AlphaComposite.SRC_OVER;
AlphaComposite AC_Rule;
AC_Rule=AlphaComposite.getInstance(
ac,tra_val);
g2d.setComposite(AC_Rule);
Set font style:
```

Step6 –*Save the watermarked BufferedImage.*

The declared type of the paintComponent argument is Graphics (Graphics2D inherits from Graphics), so first cast the Graphics object to a Graphics2D object before drawing. The composite method specifies how the pixels of a new shape are combined with the existing background pixels. The second approach permits you to set the alpha value associate with composite rule, which controls the transparency of the shape. By default, the transparency value is 1.0f (opaque).

```
Font f; f=new Font(“Arial”,
Font.BOLD, 25);
g2d.setFont(f);
To draw string on image to
bufferedimage:
String watermark; watermark=”@SCIT,
GBU”;
g2d .drawString(watermark,
(icon.getIconWidth()/4),
(icon.getIconHeight()/2));
To save watermarkedimage:
File file = fc.getSelectedFile();
try{
ImageIO.write(bid, "jpg",file);
 catch(Exception ex){}
}
```

4. Experimental Results

After implementing the algorithm following snapshots have been taken. These images show the results after watermarking. We have used Fingerprint Verification Competition 2004 as a fingerprint database for the depiction of results of watermarking. This is a public domain fingerprint database. For this purpose we have used four databases Database 1, Database 2, Database 3 and Database 4. These four databases are online accessed from the Source [46]. The fingerprints in these databases are collected with the help of different sensors and in different conditions as wet/dry impressions, rotated fingerprint, light/dark fingerprint impression etc. The complexity of proposed watermarking algorithm is O (1). Results of proposed watermarking algorithm are shown in following figures.

5. Conclusion and Future Work

This paper describes a fingerprint watermarking method in order to increase the degree of privacy of fingerprint data. Text watermarking of fingerprint image is only acceptable if it does not lead to reduced performance of fingerprint identification system. In this paper, we have designed and implemented the watermarking algorithm which provides the same accuracy of fingerprint identification system as it was providing before watermarking of fingerprint images. Experiments on a public domain fingerprint database (i.e. FVC 2004) demonstrates that the use of minutia descriptors leads to an order of magnitude reduction in the false accept rate without significantly affecting the genuine accept rate. In future we can design the new method for image watermarking of fingerprint images rather than text watermarking and corresponding performance can be evaluated with the comparison of both the algorithms. A high-resolution surface scanner was adopted for the contactless lifting of latent fingerprint. A new watermarking approach was presented and applied to fingerprint image data of such a sensor format to support a forensic investigation by privacy protection, hierarchical access and the generation of a chain of custody enabling the reproducibility of changes made to the data. Experimental results show extremely high capacities for all fingerprint samples and mixed results for standard images while meeting the required target capacities in most cases leaving a lot of additional payload or signatures. The scheme therefore is efficient for the biometric application presented.

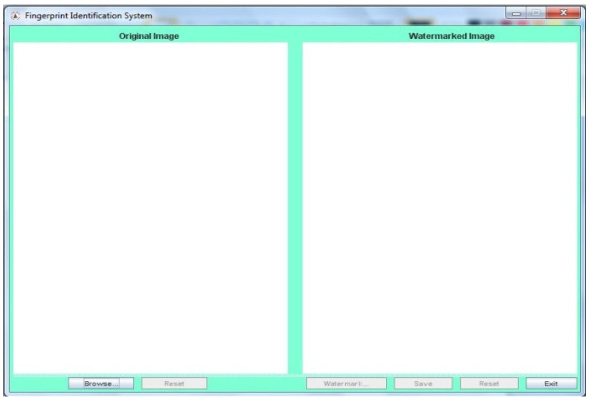
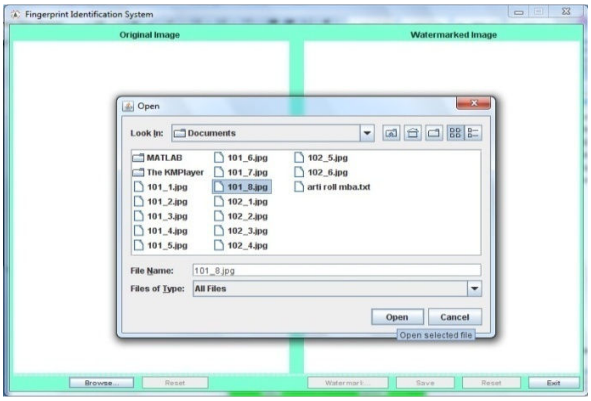
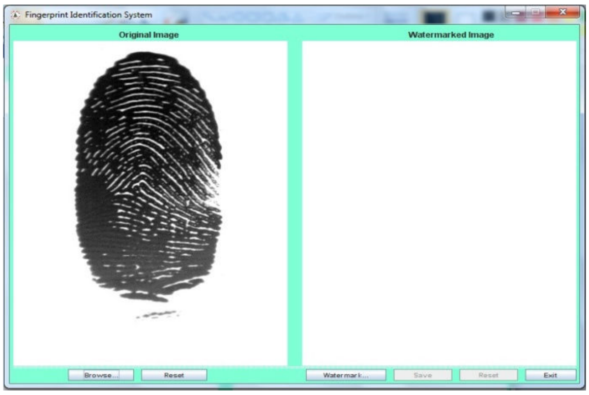


Fig 4.1: Simple GUI for text watermark image



Look In: Documents
File Name: 101_8.jpg
Files of Type: All Files

Fig 4.2: Click on browse button to open a dialog box for selecting an appropriate image



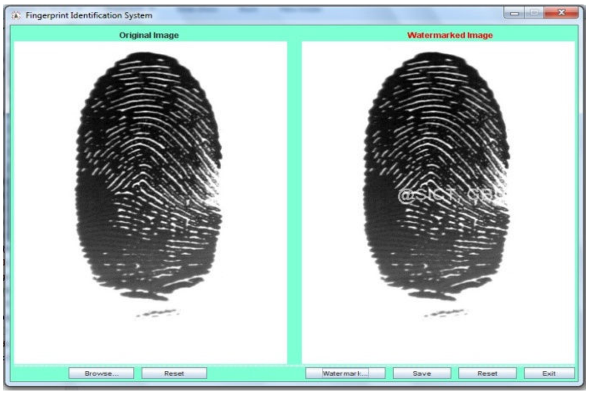
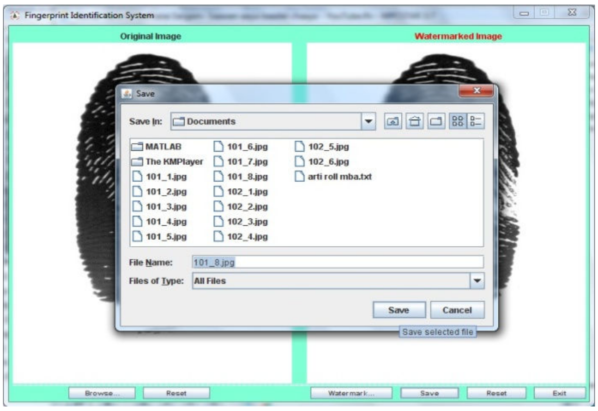


Fig 4.3: After selecting an appropriate image

Fig 4.4: Fingerprint Image after watermarking



File Name: 101_8.jpg

Files of Type: All Files

Fig 4.5: Save the text watermarked image.

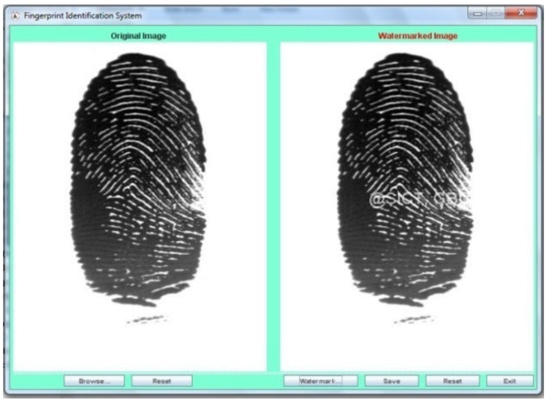


Fig 4.6: Fingerprint Image after watermarking

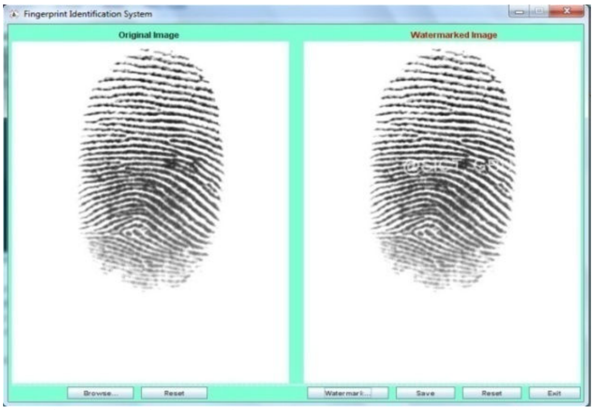


Fig 4.7: Fingerprint Image after watermarking

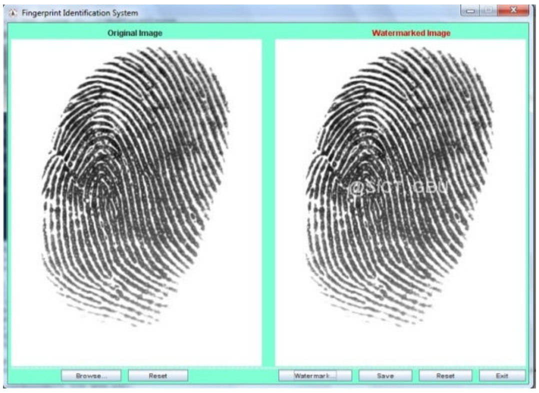


Fig 4.8: Fingerprint Image after watermarking

References

[1]. A. Z. Tirkel, G. A. Rankin, R. M. van Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne., (2000). "Electronic Watermark", DICTA Macquarie University, Sydney, pp. 666-672.

[2]. Ahmed, F. and Moskowitz, I.S. (2005). "Composite Signature Based Watermarking for Fingerprint Authentication", ACM Multimedia and Security Workshop, New York, pp. 1-8.

[3]. Chang-Hsing Lee and Yeuan-Kuen Lee., (1999). "An Adaptive Digital Image Watermarking Techniques For Copyright Protection", National Science Council of R. O. C., IEEE Transaction on Consumer Electronic, Vol. 45, No. 4.

[4]. Coatrieux, G. Lamard, M. Daccache, W. Puentes, W. Roux, C. (2006). "A Low Distorsion and Reversible Watermark: Application to Angiographic Images of the Retina", 27th Annual International Conference of the Engineering in Medicine and Biology Society, pp. 2224-2227.

[5]. Daugman J and Downing C (2001). "Epigentic randomness, complexity, and singularity of human iris patterns", Proceddings of the Royal Society, B, 268, Biological Sciences, pp 1737 – 1740.

[6]. F. M. Boland, J. J. K. O Ruanaidh and C. Dautzenberg, (1995). "Watermarking digital

images for copyright protection", Proceedings of the international Conference on Image Processing and its Applications, Edinburgh, Scotland, pp. 321- 326.

[7].http://docs.oracle.com/javase/tutorial/uiswing/components/filechooser.html.

[8].http://en.wikipedia.org/wiki/Digital_watermarking.

[9].http://en.wikipedia.org/wiki/Digital_watermarking#History.

[10]. http://www.apl.jhu.edu/~hall/java/Java2D-Tutorial.html#Java2D-Tutorial-Transparency.

[11]. http://www.apl.jhu.edu/~hall/java/Java2D-Tutorial.html#Java2D-Tutorial-Introduction.

[12].http://www.developer.com/java/other/article.php/3403921/Processing-Image-Pixels-using-Java-Getting-Started.htm.

[13].http://www.exampledepot.com/egs/java.awt.image/CreateBuf.html.

[14].http://www.watermarkingworld.com/digital_watermarking.

[15]. Hui, K., Jing, L., Xiao-dong, Z. and Xiao-xu, Z. (2008). "Study on Implementation of a Fingerprint Watermark", International Conference on Computer Science and Software Engineering (CSSE), Vol. 3, pp.725-728.

[16]. I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, (1997). "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, Vol. 6, no. 12, pp. 1673-1687.

[17]. I. J. Cox and M. L. Miller, (1997). "A review of watermarking and the importance of perceptual modeling", Proceedings of the SPIE International Conference on Human Vision and Electronic Imaging II, Feb. 10-13, San Jose, CA, USA, pp. 92-99.

[18]. I. J. Cox, (1999). "Spread-spectrum techniques for image watermarking", to appear in Proceedings of the IEEE, Special issue on identification and protection of Multimedia Information.

[19]. J. Brassil, S. Low, N. Maxemchuk, L. O' Gorman,. (1994). "Electronic marking and identification techniques to discourse document copying", Proceeding of INFOCOM.

[20]. J.J.K. O Ruanaidh, W.J. Dowling, F.M. Boland., (1996). "Watermarking Digital Image Copyright Protection", IEE Proc. - Vis. Image Signal Process, Vol. 143. No. 4.

[21]. Jain, A.K., Hong, L. and Bolle, r. (1997). "Online fingerprint verification", IEEE Trans. Pattern Anal. Machine Intell, Vol. 19, No.4, pp.302-314.

[22]. Jain, A.K., Nandakumar, K. and Nagar, A., (2008). "Biometric Template Security", EURASIP Journal on Advance in Signal Processing, Vol. 2008, Article ID 579416.

[23]. Jain, S., (2000). "Digital watermarking techniques: a case study in fingerprint & faces", Proceedings ICVGIP, pp. 139-144.

[24]. Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi and Ahmed Bouridane, (2006). "Protecting fingerprint data using watermarking", First NASA/ESA Conference on Adaptive Hardware and Systems (AHS), pp. 451-456.

[25]. Lee, Y., Kang, H.J. and Ki, Y.H (2005). "Copyright Authentication Enhancement of Digital Watermarking Based on Intellingent Human Visual System Scheme, Knowledge-Based Intelligent Information and Engineering Systems, Intelligent Watermarking Algorithms and Applications", Vol. 3682/2005, pp. 567-572.

[26]. Lin, C., (2000). “Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection”, PhD Thesis, Columbia University.

[27]. Low, C.Y., Teoh, A.B. and Tee, C. (2009). “Fusion of LSB and DWT Biometric Watermarking Using Offline Handwritten Signature for Copyright Protection”, Proceedings of the Third International Conference on Advances in Biometrics, Lecture Notes In Computer Science, Vol. 5558, pp. 786-795.

[28]. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, (1998). “Multimedia data embedding and watermarking technologies”, to appear in Proceeding of the IEEE, 1998.

[29]. M. Kutter and F. Hartung, (1999). “Image watermarking techniques”, to appear in Proceedings of the IEEE, Special Issue on Identification and Protection on Multimedia Information.

[30]. Maiorana, E., Campisi, P., Neri, A. (2007). “Biometric Signature Authentication Using Randon Transform- Based Watermarking Techniques”, IEEE Biometric Symposium, pp. 1-6.

[31]. Ms. D. Mathivadhani, Dr. C. Meena., (2010). “A Comparative Study on Fingerprint Protection Using Watermarking Techniques”, Global Journal Computer Science and Technology, Vol. 9, Page 98.

[31]. Munesh Chandra, Shikha Pandey, Rama Chaudhary, (2010). “Digital Watermarking Technique for Protecting Digital Images”, pp 12-18.

[32]. Noore, A., Singh, R., Vatsa, M. and Houck, M.M. (2009). “Enhancing security of fingerprints through contextual biometric watermarking”, Forensic Science International, Vol. 169, pp. 188-194.

[33]. Pankanti, S. and Yeung, M.M. (1999). “Verification watermarks on fingerprint recognition and retrieval”, Proc. SPIE EI, San Jose, CA, Vol. 3657, pp. 66-78.

[34]. R. B. Wolfgang and E. J. Delp, (1997). “Overview of image security techniques with applications in
multimedia systems”, Proceeding of the SPIE International Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways, November 4-5, Dallas Texas, Vol. 3228, pp. 297-308.

[34]. R. G. van Schyndel, A. Z. Tirkel, N. R. A. Mee, C. F. Osborne., (1994). “A Digital Watermark”, First IEEE ImageProcessing Conference, Houston TX, Vol. II, pp. 86-90.

[35]. Ratha, N.K., Connell, J.H. and Bolle, R.M. (2000). “Secure data hiding in wavelet compressed fingerprint images”, Proc.ACM Multimedia Workshops, Los Angeles, CA, pp. 127-130.

[36]. Ryoung, K., Jeong, D.S., Kang, .J. and Lee, E.C. (2007). “A Study on Iris Feature Watermarking on Face Data”, Proceedings of the 8th international conference on Adaptive and Natural Computing Algorithms, Part II, Lecture Notes In Computer Science, Vol. 4432, pp. 414-423.

[37]. S. Walton,. (1995). “Image Authentication for a Slippery New Age”, Dr. Dobb’s Journal, pp.18-26, 82-87.

[38]. Saraju P. Mohanty, K.R. Ramakrishna, Mohan Kankanhalli, (1999) "A Dual Watennarking Technique for Images",Proc. 7th ACM International Multimedia Conference, ACM-MM'99,Part 2, pp. 49-51.

[39]. Schaathun, H.G. (2006). “On watermarking fingerprinting for copyright protection”, Proceedings of the First International Conference on Innovative

Computing, Information and Control, IEEE Computer Society, Vol. 3, pp. 50-53.

[40]. Tzouveli, P. Ntalianis,K.. Kollias, S. (2005). “Human face watermarking based on Zernikemoments”, Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, pp. 399-404.

[41].Uludag,U.,Gunsel,B.and Ballan,M. (2001). “A spatialmethod for watermarking of fingerprint images”, Proceedings of First International Workshop on Pattern Recognition inInformation Systems, Setúbal, Portugal, pp. 26-33.

[42]. Vatsa, M., Singh, R., Noore, A., Houck, M.M. and Morris, K. (2006). “Robust biometric image watermarking for fingerprint and face template protection”, IEICE Electronics Express, Vol.3,No.2, pp. 23-28.

[43]. Zebbiche, K. and Khelifi, F. (2009). “Region-Based Watermarking of Biometric Images:Case Study in Fingerprint Images”, International Journal of Digital Multimedia Broadcasting, Vol. 2008, Article ID 492942, pp. 1-13.

[44]. Yiwei Wang, John F. Doherty, Robert E. Van Dyck, (2001). “A Watermarking Algorithm for Fingerprinting Intelligence Images”, Conference on Information Sciences and System, The Johns Hopkins University.

[45]. Yusnita Yusof and Othman O. Khalifa, (2007). “Digital watermarking for Digital Images Using Wavelet Transformation”, appear in proceeding of the IEEE pp. 665-669.

[46] http://bias.csr.unibo.it/fvc2004