Biometric System Security Issues and Challenges

Jyotika Chopra[1], Amod Kumar[2], Ashwani Kumar Aggarwal[3], Anupma Marwaha[4]
[1]*ECE, SLIET Longowal, Punjab, India*
[2]*Central Scientific Instruments Organisation, Sector 30-C, Chandigarh, India*
[3]*EIE, SLIET Longowal, Punjab, India*
[4]*ECE, SLIET Longowal, Punjab, India*
[1]jyotika.chopra1@gmail.com

***Abstract*— Biometric system finds applications in crime prevention, banking, personnel identification etc. With advancement of electronics and information technology, sophisticated biometric systems have come to existence. However, there are still many issues and challenges which need to be addressed in this area. In this paper, we give the basic modules of biometric system, enumerate the various security aspects and the methodologies to tackle them. Specifically, the role of watermarking and its implications and selection of suitable watermarking technique for a given biometric system have been discussed. Comparative study of various watermarking methods has also been done.**

***Keywords*— Biometric system, Image Processing, Signal Enhancement, Security, Watermarking, Performance indices**

I. INTRODUCTION

Biometrics use physiological as well as behavioral characteristics of human beings to secure real time systems. They are used in day to day life to ensure the represented services to be accessed only by the authorized users. Examples of physiological characteristics include DNA, ear, face, fingerprint, hand geometry, iris, and retina whereas behavioral characteristics include gait, signature, and voice. Every biometric system has its advantages as well as disadvantages.

The choice of biometric system depends upon user requirements. With the rapid growth of network distributions of digital media contents, steps must be taken first to secure the data used on internet either on mobile or somewhere else. Second, it is required to protect the data from plagiarism.

There is a solution to copyright protection problems as many digital watermarking schemes have been proposed for intellectual property right protection of digital media data [1].

II. BIOMETRIC SYSTEM

Biometric system is a technology which uses unique information about a person to identify and authenticate him on the basis of his physiological and behavioural characteristics. It is either an identification or verification system. Fig 1 below shows the block diagram of a general biometric system.

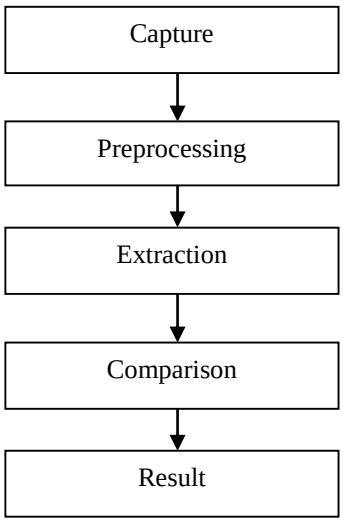


Fig. 1 Block Diagram of Biometric system

Every biometric system undergoes through four stages: Capture, Preprocessing, Extraction and Comparison.

C. Capture

First, data is collected either from online or offline resources during enrolment phase. In online collection, image is generally captured via web camera in real time. In offline basis, image is captured either via scanner or previous database kept on internet.

D. Preprocessing

Captured image (Fig 2) is processed through basic image processing steps. Image is converted into gray scale image using equation (1) below.

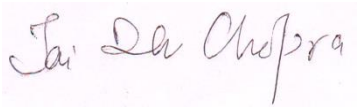


Fig 2 Color Image

$$I_g = 0.299I_C^R + 0.5871I_C^G + 0.1141I_C^B \quad (1)$$

Where $I_g$represents gray scale, I_C^R represents red component of color image, $\mathrm{I_C^G}$ represents green component of color image and $\mathrm{I_C^B}$ represents the blue component of color image.

The converted gray image is shown in Fig 3.

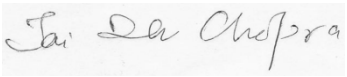


Fig. 3: Gray Image

Thresholding is then done and the image is converted into binary image (Fig 4) using equation (2).

$$I_b = \begin{cases} 1 \; if \; I_g \geq I_{Th} \\ 0 \; otherwise \end{cases} \quad (2)$$

Where I_b represents binary image, Ig represents gray image, I_{TH} represents Threshold Value (selected as 85).

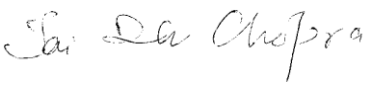


Fig. 4: Binary Image

E. Extraction

Preprocessed output is used as input for this stage. Now the main focus is on local or global feature extraction. It may be bifurcation or termination of minutiae. Unique data is extracted from the image and stored as template for the specified person.

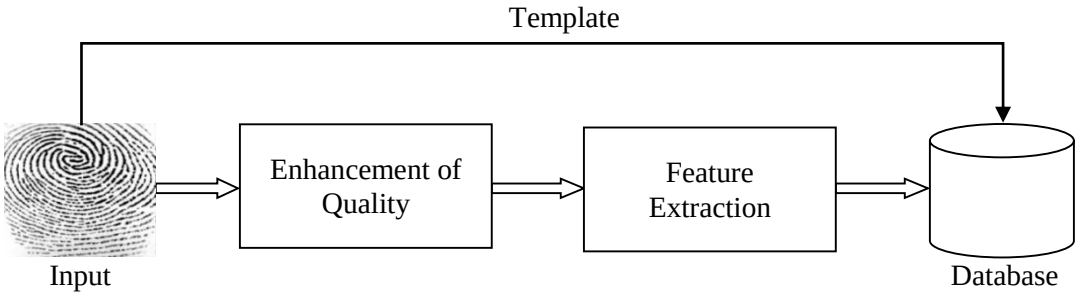
F. Comparison

The stored template is compared with new template and system decides from the output whether the features extracted from the new sample are a match or a non-match with the template.

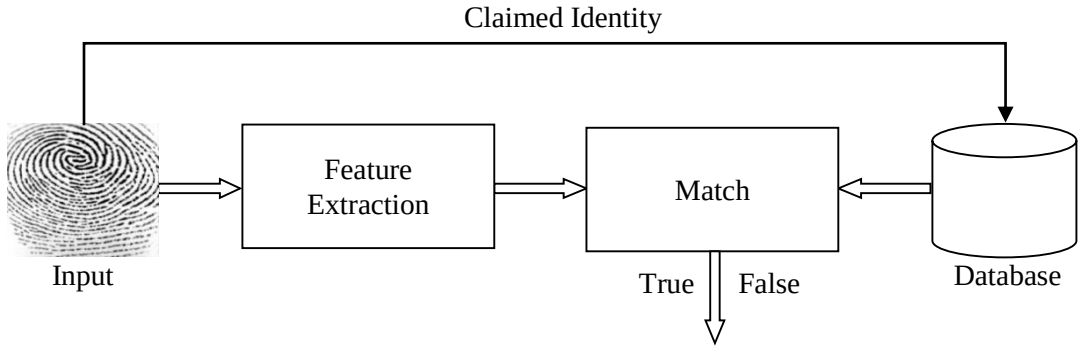
When identity needs checking, the person interacts with the biometric system for a second time, a new biometric sample is taken and passed on to the matcher. Matcher compares it with other existing templates, estimating the distance between them. If the template and the new sample match, the person's identity is confirmed [2].

The block diagram in Fig. 5 depicts the modules of every phase i.e. enrolment, verification and identification of a person. Enrolment phase takes digital image of the fingerprint as its input. The image is enhanced using an enhancement method. Features are then extracted and a database is prepared from the extracted features.

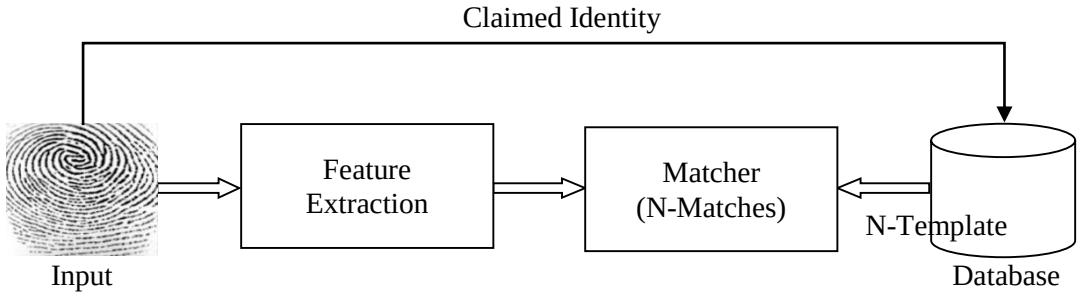
Verification phase involves template image. Extracted features are matched with features stored in the database. In the identification phase, the number of matches are seen.



ENROLMENT PHASE



VERFICATION PHASE



IDENTIFICATION PHASE

Fig. 5: Block diagrams of Enrolment, Verification and Identification

III. SECURITY OF BIOMETRIC SYSTEM

Specific algorithms or techniques have to be chosen to make biometric system Secure, Accurate and Fast (SAF). The efficient algorithm will increase the performance of the system and provide security to the system. There are various techniques by which we can secure the system. These include watermarking, cryptography, stenography etc. Encryption is good for transmission but does not provide a way to investigate the original data in its protected form. Cryptographic techniques provide matching in encrypted field. But Watermarking is the best technique to resolve some of these problems. Watermarking is a technology that has wide variety of applications, each of which may have very different requirements. Each application demands a different tradeoff between the properties of robustness, tampering, and false positive rate [2].

The aim of this technique is to protect the copyright of broadcast and exposed multimedia data. Attackers have the freedom to obtain copies of copyrighted electronic material via the Internet and change them. Watermarking is the most popular method to protect copyright information [3]. The main requirements for an acceptable technique of watermarking is discussed in [4]. A watermarking scheme consists of three parts: the watermark, the encoder, and the decoder. An algorithm is required to combine the watermark with the object, whereas verification algorithm authenticates the object by determining the presence of the watermark and its actual data bits and various transforms such as Fourier, Wavelet transform etc are used to embed the watermark. Long back, watermarking was more or less a transparent image was applied to a piece of paper. Its application in electronics

information field involves hiding secret information in the digital images that allows invisible mark to be placed on top of normal information such as bank note, ID card and other valuable documents. The applications of watermarking are broadcast monitoring, transactional watermarks, copy control and covert communication. Watermarking is a robust technique because it has potential to survive against hackers [5].

In paper [6], authors proposed novel digital watermarking technique using face and demographic text data as multiple watermarks. Fingerprints are one of the reliable biometric identifiers that are used for person authentication. Fingerprint is verified through matching score. The watermarked fingerprint adds protection from tampering and the fingerprint matching ability is not affected. For the extraction of embedded face and text, original images are not required.

In [7], the author proposed a blind data hiding method which is applicable to fingerprint images compressed with wavelet-packet scalar quantization. Paper [8] describes the CS Theory framework in wavelet domain for security and authentication of biometric template. DWT is used to maintain the high quality of fingerprint image after embedding two biometric modalities. In paper [9], a spread-spectrum-like discrete cosine transform domain (DCT domain) watermarking technique is used for the analysis of still digital images. For this purpose, first stage image was not used as it is generally corrupted by noise. Gaussian distribution was assumed used for statistically modelling of noise. The DCT coefficients of the image show how the resulting detector structures lead to considerable improvements in performance with respect to the correlation receiver. Existing algorithms for watermarking still images usually work either in the spatial domain [10, 11, 12, 13] or in frequency domain [14, 15]. Frequency domain methods are robust to several kinds of attacks such as compression, filtering, scaling, cropping, and rotation etc. In paper [16], author discuss major problem in Rotation, scaling, and translation (RST)-invariant watermarking. The algorithm is combination of both frequency domains watermarking with spatial-domain watermarking (SW) based on quantisation strategy. It is not only robust to RST but also helps to eliminate computational complexity.

In paper [17], author composes a self embedding watermarking scheme in spatial domain for color images to achieve temper proofing and high quality recovery. In paper [18], author discusses privacy issues related to data mining by using a user-role based methodology. It focuses privacy-preserving mining of data usually by removing or replacing sensitive information from the original data. In paper [19], author proposed a novel rank based method for image watermarking in the discrete cosine transform (DCT) domain. The two DCT coefficients are used to embed one watermark bit. This technique is free of host signal interference (HSI) and has high robustness against attacks. Paper [20] proposed a novel robust audio watermarking method based on the time-spread (TS) echo hiding scheme.

In [21], proposed a genetic algorithm for parameter optimization to maximize the imperceptibility and robustness in which two-level discrete wavelet transform (DWT) is applied to the original image for embedding a binary watermark. In paper [22], author encrypted the logo into a random noise signal for security where the logo is embedded into the mid-frequency redundant discrete wavelet transform (RDWT) sub bands . A novel quantization watermarking method (NCQM) is introduced in paper [23]. The normalized correlation (NC) is calculated between the host signal and a random signal. Modulation is carried out by selecting a codeword from the codebook associated with the embedded information. The technique achieves the improved watermark imperceptibility but also is more robust to a wide range of attacks i.e. e.g., Gaussian filtering, additive noise etc. A robust lossless watermarking is proposed in [24] in which data is recovered correctly after the hidden data extraction and the hidden data is robust against attacks. The pixel adjustment process is applied as a post-processing step, which helps in improving the image quality and obtaining a completely reversible watermarking (RW) scheme. A robust lossless relational database watermarking scheme is proposed in [25] in which circular histogram modulation is used. It is used for verifying the integrity and the authenticity of the database even if the database has been modified. Its results allow the user to correctly select the scheme parameters under limitation of robustness and distortion.

In paper [26], multipurpose mechanisms based on the multiscale curvelet transform is presented to realize copyright protection and content authentication simultaneously. The new methodology is applied in [27] to spread spectrum schemes where theoretical and practical calculations of the effective key length are proposed. This measure is similar to the brute force attack in cryptography, but difference is there will not be unique key which granting access to watermarking channel.

IV. CONCLUSION

Biometric systems are used in our day to day life and lot of research has gone into this area but still there are some issues and challenges that are discussed in this paper. Security is the main focus of discussion. For example, the biometric key we are using may be stolen by unknown person. A biometric system which is based either on physiological or behavioural characteristics of a person can always fail when an intruder tries to manipulate the data by modifying its contents as the manipulated data causes the biometric system to lead to false final decision. Such issues are a matter of great concern and pose a question as to how we can design the system effectively so that hackers and attackers are not able to disturb the internal as well as external working of biometric system. To overcome this problem, system must be designed in such a way that the behavioural characteristics are periodically monitored. This process will help in detecting the risks of potential attacks. Any change in the behavioural characteristics must be communicated to the system. At the same time, accurate and precise decision should be taken to replace the software component with hardware implementation as far as possible.

Besides this, a technique which will improve the performance of the biometric system is watermarking. We have cited few research works describing various facets of watermarking technique which ensure the efficient hiding of data on the basis of some coding or key applied to biometric technique successfully.

ACKNOWLEDGMENT

We owe our special thanks to Director SLIET, Longowal for extending computational facilities for this work.

REFERENCES

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, NY, 2003
[2] Gonzalez, R.C., Woods, R.E.: Digital image processing (Prentice Hall, 3rd ed., 2007)
[3] Athanasios Nikolaidis and Ioannis Pitas, "Region-Based Image Watermarking" , *IEEE Transactions On Image Processing*, Vol. 10, No. 11, November 2001, pp 1726-1740
[4] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: A framework", *IEEE Comput. Graphics and Applications*. Vol. 19, No. 1, January/February1999 pp. 18–24
[5] R. Ashoka Rajan, R. Angelinjosphi, Ms. PVS Gayathi, T. Rajendran, P. Anandhakumar", A Novel Approach for Secure ATM Transactions Using Fingerprint Watermarking", *Fifth International Conference on Advanced Computing (ICoAC), 2013*
[6] Afzel Noore, "Enhancing security of fingerprints through contextual biometric Watermarking", available online at *sciencedirect.com Forensic Science International* 169 (2007), pp. 188–194
[7] N.K. Ratha, J.H. Connell, R.M. Bolle, Secure data hiding in wavelet compressed fingerprint images, in: *International Multimedia Conference, Proceedings of ACM Workshop on Multimedia*, 2000, pp. 127–130
[8] Rohit M. Thanki, Komal R. Borisagar, "Compressive Sensing Based Multiple Watermarking Technique for Biometric Template Protection", *I.J. Image, Graphics and Signal Processing*, 2015, 1, pp. 53-60. Published Online December 2014 in MECS (http://www.mecs-press.org/). DOI: 10.5815/ijigsp.2015.01.07
[9] Juan R. Hernández, Martín Amado, Fernando Pérez-González, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", *IEEE Transactions on Image Processing*, Vol. 9, No. 1, January 2000, pp. 55-68
[10] M. D. Swanson, B. Zhu and A. H. Tewfik, "Robust data hiding for images", *Proc. IEEE Digital Signal Processing Workshop*, Loen, Norway, Sept. 1996, pp. 37–40
[11] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection", in *Proc. Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, R. Oldenbourg, Ed., Vienna, Austria, Aug. 21–25, 1995, pp. 242-251
[12] R. B. Wolfgang and E. J. Delp, "A watermark for digital images", *Proc. 1996 Int. Conf. Image Processing*, Vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 219–222
[13] J. R. Smith and B. O. Comiskey, "Modulation and information hiding in images, " *Proc. Int. Workshop on Information Hiding*. Cambridge, UK, May 1996, pp. 207–226
[14] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia*", IEEE Trans. Image Processing*, Vol. 6, Dec. 1997, pp. 1673–1687
[15] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection", *Proc. Inst. Elect. Eng. Conf. Vision, Image and Signal Processing*, Vol. 143, Aug. 1996, pp. 250–256
[16] Y. T. Lin , C. Y. Huang , G. C. Lee, "Rotation, scaling, and translation resilient watermarking for images", *IET Image Processing*, Vol. *5*, Iss. 4, Jun 2011, pp 328-340. DOI: 10.1049/iet-ipr.2009.0264.
[17] K.-C. Liu, " Colour image watermarking for tamper proofing and pattern-based recovery, " *IET Image Processing*, Vol. *6*, Iss. 5, 2012 , pp 445-454. DOI: 10.1049/iet-ipr.2011.0574.
[18] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, ``Information security in big data: Privacy and data mining, *" IEEE Access*, vol. 2, pp. 1149-1176, 2014
[19] Y. Xiang et al, " Rank-Based Image Watermarking Method With High Embedding Capacity and Robustness, " in *Special Section On Latest Advances And Emerging Applications Of Data Hiding* , May 9, 2016.. Digital Object Identifier 10.1109/ACCESS.2016.2556723
[20] Peng Hu, " Robust time-spread echo watermarking using characteristics of host signals, " Electronics Letters , 8th January 2016, Vol. 52 No. 1 , pp. 5-6.
[21] K. Ramanjaneyulu and K. Rajarajeswari, "Robust and obivious image watermarking scheme in the dwt domain using genetic algorithm, " *Int. J. Advanced Eng. Technology* , vol. 2, no. 3, pp. 85–92, 2011.
[22] T. D. Hien, Z. Nakao, and Y. W. Chen, "Robust multi-logo watermarking by rdwt and ica, " *Elsevier journal of Signal Processing*, Vol. 86, pp. 2981–2993, 2006
[23] Xinshan Zhu et al , "Normalized Correlation-Based Quantization Modulation for Robust Watermarking, " *IEEE Transactions on Multimedia*, Vol. 16, No.7, pp 1888-1904 November 2014.
[24] Rasha Thabit et al , "Capacity improved robust lossless image watermarking, "IET Image Processing 2014, Vol. 8, Iss. 11, pp. 662–670 doi: 10.1049/iet-ipr.2013.0862.
[25] Javier Franco-Contreras et al, "Robust Lossless Watermarking of Relational D.atabases Based on Circular Histogram Modulation, "*IEEE Transactions on Information Forensics And Security*, Vol. 9, No. 3, pp 397-410 March 2014
[26] Chune Zhang et al , " Multipurpose Watermarking Based on Multiscale Curvelet Transform, " *IEEE Transactions On Information Forensics And Security*, Vol. 3, No. 4, pp 611-619, December 2008.
[27] Patrick Bas et al , "A New Measure of Watermarking Security: The Effective Key Length, " *IEEE Transactions on Information Forensics and Security*, 2013, Volume: 8, Iss: 8 , pp 1306 - 1317, DOI: 10.1109/TIFS.2013.226796